МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ
ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

XII НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

„Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв'язку та автоматизації в операції Об'єднаних сил"

14 – 15 листопада 2019 року

(Доповіді та тези доповідей)

Київ – 2019

ББК
Ц4 (4Укр)39
П-768

У збірнику матеріалів дванадцятої науково-практичної конференції опубліковано доповіді та тези доповідей вчених, науково-педагогічних та наукових працівників, докторантів, ад'юнктів, здобувачів, курсантів Військового інституту телекомунікацій та інформатизації та інших вищих навчальних закладів, представників промисловості в яких розглядаються пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення, застосування підрозділів, комплексів, засобів зв'язку та автоматизації в операції Об'єднаних сил.

ЗМІСТ

1.	**Авдєєнко Г.Л., Денисенко Н.І.** Безпроводова система зв'язку на базі використання UWB трансиверів DWM1000	15
2.	**Александров О.В., Сімонов С.І.** Проблемні питання інформаційно-технічного спряження сучасних комплексів засобів автоматизації з рухомими об'єктами управління за допомогою радіостанцій УКХ-діапазону	17
3.	**Ананьїн В.О., Саєнко О.Г.** Парадигмальні засади формування особистості сучасного військового фахівця	18
4.	**Ананьїн О.В., Саєнко О.Г.** RFID-пристрої, які використовуються у сучасних паспортних документах	20
5.	**Ангелов Ю.С., Симоненко О.А.** Модель відмовостійкого об'єктного сховища за допомогою технології *CEPH*	21
6.	**Арсенович А.Д., Іващук Д.І., Тимошишин Н.М.** Перспективи застосування азбуки Морзе у військах зв'язку	22
7.	**Артюх С.Г., Лазоренко Є.М.** Аналіз безпеки систем моніторингу та спостереження за сервісами ІТС ЗСУ	23
8.	**Бабарика А.О., Катеринчук І.С., Табенський С.М.** Застосування алгоритмів розпізнавання образів на основі нейромережевих технологій	24
9.	**Баканов В.С., Чевардін В.Є.** Перспективи розвитку інформаційних мереж ЗС України	26
10.	**Барановський О.М., Жилін А.В., Новіцький І.Ю.** Методика виявлення злоякісного трафіку на основі поведінкового аналізу	27
11.	**Барановський О.М., Жилін А.В., Пилипенко О.В.** Метод виявлення фейкових базових станцій на основі аналізу параметрів перевибору станцій та радіоелектронної обстановки	28
12.	**Бардін О.О., Немченко О.О.** Перспективи застосування боєприпасів типу „Ударне ядро" для самозахисту сухопутних бойових платформ	29
13.	**Басанець Д.О., Кирган О.О.** Програмне забезпечення аналізу статистичних даних з обліку матеріальних засобів у квартирно-експлуатаційній службі	32
14.	**Безносенко С.Ю., Добропас Б.І., Білий О.А., Пономаренко З.М.** Шляхи удосконалення системи метрологічного обслуговування військ зв'язку	33
15.	**Бессалов А.В., Ковальчук Л.В., Кучинська Н.В., Теліженко О.Б.** Обґрунтування криптографічної стійкості алгоритму інкапсуляції ключа, що пропонується до стандартизації	36
16.	**Білан А.М., Жук О.В., Стемпковська Я.А., Дука О.В.** Класифікація кіберзлочинів у сучасних умовах розвитку кіберпростору	37
17.	**Білаш О.В., Глова Т.Я., Сорокатий М.І.** Вдосконалення підготовки військових фахівців на основі інтенсифікації практичного заняття	38
18.	**Бірюков П.В.** Досвід навчання військових фахівців США у синтетичному віртуальному середовищі	40
19.	**Бовда В.Е.** Петрі-об'єктна модель транспортних перевезень матеріальних засобів у військових підрозділах	42
20.	**Бовда Е.М.** Бойове застосування підрозділів зв'язку з урахуванням досвіду операції Об'єднаних сил	43
21.	**Бойко О.В., Буяло О.В., Пилипчук В.В.** Методика модифікації операційної системи Android на мобільних пристроях для запобігання передачі статистичної інформації	45
22.	**Бондаренко Л.О., Бондаренко О.Є., Бузаєва К.О., Руденко В.І.** Управління телекомунікаційною інфраструктурою Збройних сил України: стан, задачі, підходи і перспективи	46
23.	**Борисов І.В., Березанський Д.О., Петрова Д.В.** Обґрунтування і сутність методики обробки сигналів в системі MIMO при впливі навмисних завад	48
24.	**Бруяка Р.В., Грохольський Я.М.** Варіант модернізації телекомунікаційного комплекту тип-1	50
25.	**Бугайов М. В., Калетинець Р. В.** Методика визначення параметрів радіопередач зі швидкою програмною перебудовою робочої частоти та частотною маніпуляцією	51
26.	**Василенко С.В.** Кодування синхромітки підсистеми входження в синхронізм системи радіозв'язку з псевдовипадковим перенаналаштуванням робочої частоти	53
27.	**Василишин В.І., Лютов В.В.** Оцінювання передаточної характеристики каналу зв'язку в OFDM-системах з використанням методу SSA	54
28.	**Власенко О.В., Горгуленко В.А., Андрусенко В.В.** Застосування систем керування базами даних *NOSQL* в створенні інформаційних систем ЗСУ	55
29.	**Власенко О.В., Горгуленко В.А.** Застосування систем керування базами даних *NOSQL* для модернізації військових інформаційних систем	56

30.	**Войтович М.І., Ліщинська Х.І., Пак Р.М., Сеник А.П.** Впровадження дистанційних форм навчання для вдосконалення підготовки військових фахівців	57
31.	**Голуб'ятніков А.С., Блозва А.І.** Брандмауери – основа мережевої безпеки	58
32.	**Горбенко В.І., Мартошенко М.В.** Навчально інформаційна підсистема з дисципліни „системне програмування та архітектура комп'ютера"	60
33.	**Горбенко В.І., Сачок О.М.** Підсистема обліку засобів обчислювальної техніки навчально-лабораторного комплексу кафедри ВВНЗ	61
34.	**Горбенко І.В., Харламов Є.М.** Підсистема моніторигну інформаціної системи спеціального призначення з використанням веб-технологій	62
35.	**Горлинський В.В., Ананьїн В.О.** Вдосконалення підготовки військових фахівців: безпековий аспект	63
36.	**Грачов О.В.** L3HARRIS -результати та нові перспективи	64
37.	**Гребенюк О.П., Мартинчук О.О., Роговець М.А., Гребенюк О.О.** Застосування поляризаційно-просторової обробки сигналів джерел радіовипромінювання при дії завад в засобах радіомоніторингу з антенами подвійної поляризації	66
38.	**Гуржій П.М., Коваленко І.Г., Гуржій І.А.** Аналіз функціональних можливостей спеціалізованого програмного забезпечення ведення реєстрів радіоелектронних засобів та визначення їх електромагнітної сумісності	67
39.	**Гурський Т.Г.** Підвищення завадозахищеності повітряних ретрансляторів УКХ радіомереж в умовах навмисних шумових завад	69
40.	**Давіденко С.В., Бойчук Б.М.** Принципи конвергенції телекомунікаційних мереж	77
41.	**Давидов А.А.** Визначення показника ефективності функціонування системи радіосвітлотехнічного забезпечення тактичної авіації в районі аеродрому	78
42.	**Демідов Б.О., Капранов О.В., Кучеренко Ю.Ф., Ткачов А.М.** Автоматизована система управління міжвидовим угрупованням, як одна з складових основ його боєздатності	79
43.	**Дніпровська А.М., Жук П.В.** Перспективні напрямки розвитку багатофунконального автоматизованої системи РЕБ Збройних сил України	81
44.	**Драглюк О.В., Шкорупський В.М. Ревуцький В.А.** Програмний комплекс підтримки прийняття рішень при плануванні зв'язку „Ресурс-С" можливості та порядок використання	83
45.	**Духанов М.А.** Нові та перспективні види роботи та програмне забезпечення техніки зв'язку L3HARRIS	87
46.	**Дюков І.М.** Алгоритм виявлення та формування радіоперешкод лініям радіозв'язку з широкосмуговими сигналами	88
47.	**Єрохін В.Ф., Ірха М.С.** Методика і результати аналізу завадостійкості демодулятора ФМ-сигнала з компенсацією подібної переривчастої завади	89
48.	**Животовський Р.М.** Методологічні основи управління радіочастотним ресурсом систем радіозв'язку спеціального призначення	91
49.	**Жук О. Г.** Метод формування канальних сигналів в системах з OFDM	92
50.	**Журавський Ю.В., Шишацький А.В.** Методологічні основи оцінювання радіоелектронної обстановки на основі нечіткої кластеризації часових рядів	93
51.	**Зав'ялов М.О., Гріньков В.О.** Організація мережевої розвідки засобами інтернет сервісів	94
52.	**Зайцев О.В.** Методичний підхід до визначення переваг гіпотез, представлених у вигляді конкуруючих інтервальних оцінок	95
53.	**Залевський В.Й.** Закриття телекомунікаційних каналів зв'язку з безпілотним літальним апаратом	96
54.	**Зарубенко А.О., Палівода В.С., Мартинюк А.В.** Стан та перспективи використання засобів радіозв'язку в Збройних силах України	97
55.	**Здоренко Ю.М., Кузнєцов Д.Р.** Методи обробки великих даних в інформаційних системах військово-медичних закладів	98
56.	**Здоренко Ю.М., Лаврут О.О., Диган Д.І.** Метод аналітичної обробки даних про параметри трафіку комп'ютерної мережі	99
57.	**Зроль С.С., Троцько О.О.** Аналіз безпечного мережевого доступу на базі платформи Cisco Ise	100
58.	**Івченко М.М., Ткач В.О., Мусієнко В.А., Шугалій О.О., Очіченко Р.А.** Аналіз існуючих проблем щодо забезпечення ЗІП сучасних засобів зв'язку та автоматизації	101
59.	**Іщенко Д.А., Кирилюк В.А.** Модель дезорганізації управління військами (силами) за прогнозованими варіантами комплексного застосування противником засобів вогневого ураження та радіоелектронних перешкод	103
60.	**Камак Д.О., Руденко О.В., Скиба О.В., Доманов І.О.** Проблеми в розробленні сучасних апаратних зв'язку	105
61.	**Камак Д.О., Руденко О.В., Скиба О.В., Троцик С.М.** Застосування спеціальних	106

	інформаційно-телекомунікаційних засобів для підтримки антитерористичних дій на військових об'єктах	
62.	**Карасенко І.О.** Інтеграційна платформа Дельта – новий вид збору інформації	108
63.	**Кізло Л.М., Радзіковський С.А., Жук О.В.** Сучасні напрями вдосконалення процесу підготовки військових фахівців	109
64.	**Коваль І.О., Симоненко О.А., Троцько О.О.** Зберігання даних в CEPH FS з використанням шлюзу CEPH RADOS	111
65.	**Колесник В.В.** Метод багатофакторної ідентифікації користувачів на об'єктах військового призначення	112
66.	**Колтовсков Д.Г.** Методи побудови розвід- та завадозахищених каналів управління тактичних БпЛА	113
67.	**Коновець В.І.** Деякі аспекти безпеки інформаційної взаємодії з сенсорами у складі системи спостереження за надводною обстановкою	115
68.	**Коркін О.Ю., Дідик В.О., Симоненков В.М.** Побудова ефективних інформаційно-управляючих систем у складі наземних роботизованих комплексів на підтримку мережецентричних сценаріїв бойових дій	116
69.	**Котюбін В.Ю., Романов О.М.** Алгоритм пошуку періоду цифрової послідовності на основі синхронного накопичення	118
70.	**Кротов В.Д.** Аналіз підходів моделювання трафіку з точки зору відповідності мережам тактичної ланки управління	120
71.	**Кубрак О.М.** Програмно-апаратні засоби обробки радіосигналів та формування радіоперешкод	121
72.	**Кувшинов О.В., Зотова І.Г., Боголій С.М.** Синтез високоефективних сигнально-кодових конструкцій з турбо-кодами	122
73.	**Кузавков В.В., Зарубенко А.О.** Методика синтезу цифрового коректуючого пристрою системи автоматичного управління положенням платформи антенного поля мобільної базової станції	123
74.	**Кузнецов О.О., Ковальчук Д. Ю., Дьяченко А.С., Сафоненко В.Е., Даценко С.С.** Швидкодія алгоритмів гешування, придатних для використання в блокчейн-мережах	124
75.	**Леонтович С.П.** Погляди на напрями автоматизації процесів розрахунків із логістичного забезпечення Збройних сил	126
76.	**Лисенко О.І., Явіся В.С., Петрова В.М.** Вибір способу одержання керуючої інформації системою стабілізації руху наносупутників	129
77.	**Лисенко О.І., Явіся В.С., Явіся Д.В.** Система орієнтації телекомунікаційних наносупутників	131
78.	**Лівенцев С.П., Павлов В.П., Василюк Ю.С., Ляшенко Г.Т.** Алгоритм сліпої обробки оцінювання скалярних та векторних каналів при декодуванні турбокодів в каналах із структурними завадами	133
79.	**Ліщинська Х.І., Сокіл М.Б., Сокульська Н.Б., Сеник А.П.** Організація інформаційних систем з використанням спеціалізованих математичних методів	134
80.	**Мазулевський О.Є., Саченко А.П., Толстих В.А.** Аналіз можливостей IPS рівня мережі	135
81.	**Макарчук І.М., Скиба С.Є.** Інформаційна система автоматизації процесів роботи науково-технічної бібліотеки ВВНЗ в рамках Коха	136
82.	**Макарчук В.І., Мартинюк В.В., Паламарчук С.А., Карпенко А.О.** Аналіз процесу планування зв'язку в Збройних силах України та НАТО	137
83.	**Маковейчук О.М., Рубан І.В., Худов Г.В.** Новий тип маркерів доповненої реальності	139
84.	**Марилів О.О., Мєшков С.І.** Прогнозування інтервалів часу доби для використання безпілотних літальних апаратів, обладнаних тепловізійними системами спостереження	140
85.	**Марфін О.В., Симоненко О.А.** Аналіз застосування фреймворків для розробки WEB-додатків	141
86.	**Масесов М.О.** Перспективи розвитку військових транспортних телекомунікаціних мереж	142
87.	**Машкін О.О.** Алгоритм структурної адаптації комплексів математичних моделей операцій (бойових дій) в умовах часових обмежень на отримання результатів розрахунків	143
88.	**Микусь С.А., Войтко О.В., Мазулевський О.Є.** Основні напрями протидії гібридним загрозам у кіберпросторі (через кіберпростір) Міністерством оборони та Збройними силами з урахуванням стандартів НАТО	144
89.	**Мирончук О.Ю., Шпилька О.О.** Моделювання каналів зв'язку із заданими кореляційними властивостями	146
90.	**Михалевич В.Е.** Підхід до моделювання інформаційно-телекомунікаційного забезпечення АСУ в операції оперативного угруповання військ	148
91.	**Михальчук І.І., Стаценко В.І.** Адаптивна система автоматизованої перевірки (тестування) знань курсантів	149
92.	**Могилевич Д.І., Кононова І.В.** Аналіз методів підвищення надійності програмного забезпечення систем управління військами та озброєнням	150

93.	**Могилевич Д.І., Кононова І.В.** Методика організації технічного обслуговування складної технічної системи	152
94.	**Молдован В.Д., Кінах М.О.** Захист інформації в сучасних смартфонах з операційною системою ANDROID	153
95.	**Мороз А.А., Нерознак Є.І.** Реалізація віддаленого адміністрування мережевого та серверного обладнання	154
96.	**Нагорнюк О.А., Колос Ю.О.** Вплив конструктивних рішень компонування та похибок у виготовленні елементів широкосмугової рупорної антени на її технічні характеристики	155
97.	**Назаренко І.М., Троцько О.О.** Модель системи реагування на інциденти в мережі на основі програмного стеку ELK	156
98.	**Нерознак Є.І., Кравченко А.О., Сова О.Я.** Аналіз методологій, архітектурних рішень та інструментарію розробки інформаційних систем та АСУ мережевими інфраструктурами	157
99.	**Нестеренко М.М., Баюра А.І.** Програмний модуль адаптивної побудови моделі для *3D* друку за технлогією *FDM*	162
100.	**Нестеренко М.М., Богуцький В.В.** Віртуально-тренажерний комплекс „Телекомунікаційний комплект ТИП-1" на основі програмного середовища *UNITY3D*	163
101.	**Нестеренко М.М., Ткаченко Б.О.** Програмний модуль конфігурування та управління сегментом віртуальної мережі SDN	165
102.	**Нестеров О.М., Зінченко І.А., Зінченко М.О.** Метод оцінки пропускної спроможності системи зв'язку спеціального призначення на основі дендрограми з типовими модулями зв'язку	166
103.	**Овсяннiков В.В., Гаврилюк О.Г., Черниш Ю.О.** Реалізація послуги „Ідентифікація і автентифікація при обміні" в міжнародних стандартах	167
104.	**Овсяннiков В.В., Паламарчук Н.А., Паламарчук С.А., Чередниченко О. Ю.** Підходи до формування вимог із захисту інформації від несанкціонованого доступу під час розробки програмного забезпечення для автоматизованих систем	168
105.	**Оксьоненко М.П., Яковлєв С.В.** Методи виявлення прихованих фейстель-подібних перетворень	170
106.	**Ольшанський В.В., Кухар І.Г., Єгоров Ю.А.** Автоматизована система управління „Кропива"	171
107.	**Остапук О.І., Гришина Н.С., Карабань О.В., Побережець Т.В.** Варіанти вирішення інформаційної безпеки в мультисервісній мережі зв'язку	172
108.	**Орлов В.В., Симоненков В.М.** Розвиток пасивних систем звукової локації безпілотних літальних апаратів в умовах терористичних загроз	175
109.	**Павленко К.І.** Перспективи розвитку інженерних боєприпасів в умовах ведення гібридних війн	176
110.	**Павленко О.А.** Напрямки запровадження систем імітаційного моделювання під час підготовки військових фахівців	177
111.	**Пащетник В.І., Пащетник О.Д.** Міждисциплінарна інтеграція знань у вищому військовому навчальному закладі	179
112.	**Пащетник О.Д., Живчук В.Л., Поліщук Л.І.** Розробка онтологічної системи підтримки прийняття рішень командирів тактичної ланки управління сухопутних військ Збройних сил України	180
113.	**Пилипчук Ю.В., Петров Д.В., Остапук А.І., Гетьман А.В.** Сучасні тенденції розвитку інформаційних систем в Збройних силах України	181
114.	**Пилипчук В.В.** Метод виявлення рухомих морських об'єктів на цифрових знімках видових засобів	185
115.	**Півторайко І. В., Лахно В. А.** Виявлення аномалій за допомогою зовнішнього (outlier) підходу	186
116.	**Погребняк Л.М., Кононова І.В.** Ефективність завадостійкого та просторового кодувань в нестаціонарних частотно-селективних каналах систем військового радіозв'язку	188
117.	**Подліпаєв В.О., Хижняк І.А.** Аналіз сучасних геоінформаційних систем щодо трансдисциплінарного використання слабоструктурованих даних	189
118.	**Покотилюк О.О., Стоцький І.В.** Програмний модуль обрахунку можливих наслідків ядерного вибуху	191
119.	**Поліський О.М.** Методика фільтрації оцінок елементів вектору стану при умові рівномірного прямолінійного руху цілі	192
120.	**Полуяненко М.О., Онікійчук О.О., Деменко Є.Є., Гончаров М.О., Писаренко Н.В.** Оцінка ймовірності подвійних витрат в блокчейн системах на підставі „моделі незалежних гравців"	193
121.	**Почерняєв В.М., Помін А.Г., Колодійчук Л.В.** Радіорелейна компонента мобільної цифрової тропосферно-радіорелейної станції	185
122.	**Пушкарьов Ю. О., Ревенко В.Б.** Метод синтезу слідкувальних автоматичних систем управління підвищеної точності	197
123.	**Рибка С.В., Корольов А.П., Варава І.А.** Програмний засіб проектування цифрових фільтрів	198

	методом частотної вибірки	
124.	**Рижов Є.В., Сакович Л.М.** Метод розподілу часу при відновленні радіоелектронних засобів з кратними дефектами	199
125.	**Рихальський О.Р., Натальчук С.В.** Оцінка впливу параметрів каналу зв'язку на якість передачі інформації в рухомих системах стандарту GSM	200
126.	**Романенко І.О.** Аналіз завдань і методів оцінки та вибору альтернатив рішень	201
127.	**Романюк В.А.** Алгоритм позиціонування телекомунікаційних аероплатформ для збільшення пропускной здатності повітряної мережі	203
128.	**Руденко В.І., Бондаренко Л.О., Бузаєва К.О., Остапук О.І.** Перспективи розвитку тропосферного зв'язку у Збройних силах України	208
129.	**Руденко М.М., Симоненко О.А.** Модель організації системи візуалізації Kibana в мережах спеціального призначення	210
130.	**Руцький В.О., Троцько О.О.** Аналіз засобів віддаленого автоматизованого управління мережевою інфраструктурою	211
131.	**Самойлов І.В., Застело Г.І.** Використання елементів штучного інтелекту для видобування нечітких відношень з експериментальних даних	212
132.	**Семенов А.О. Троцько О.О.** Аналіз дестабілізуючих факторів, що впливають на функціонування мереж передачі даних спеціального призначення	213
133.	**Сердюк П.Є., Слюсар В.І.** Технології доповненої реальності – сучасний стан та перспективи	214
134.	**Сидорчук О. Л., Кліменко Д.О., Дворський В. О.** Малогабаритний рупорний опромінювач дзеркальних антенних систем станцій радіотехнічної розвідки	215
135.	**Сидорчук О. Л., Левунець Р. О.** Дослідження електромагнітного поля для проектування дзеркальних антенних систем станцій радіотехнічної розвідки	216
136.	**Симоненко О.А., Білан А.М., Жук О.В.** Кібертероризм у контексті побудови системи кібернетичного захисту держави	217
137.	**Слюсар В.І.** Концепція архітектури транспортних засобів як мережі мереж	218
138.	**Слюсар Є.А., Редзюк Є.В.** Програмний модуль аналітичної обробки даних успішності навчальних груп	220
139.	**Сокульська Н.Б., Сокіл Б.І., Ковальчук Р.А., Кмін В.Ф.** Дистанційне навчання як один із напрямів вдосконалення підготовки військових фахівців	221
140.	**Солодовник В.І., Висоцька Т.М., Османов Р.Н.** Оцінка завадостійкості методів просторового кодування сигналів з дворежимною індексною модуляцією піднесучих	223
141.	**Сорокатий М.І., Петрученко О.С., Білаш О.В.** Специфіка викладання вищої математики у ВВНЗ	225
142.	**Степаненко Є.О.** Оцінка ефективності методик управління топологією наземно-повітряних радіомереж	227
143.	**Ступак Д. Є.** Методика оцінювання ефективності функціонування системи гарантування якості вищої військової освіти	231
144.	**Сусь Б.А., Грохольський Я.М.** Фізичний зміст поняття „струм зміщення"	233
145.	**Тарара В.М., Нерознак Є.І.** Реалізація віддаленого доступу до комп'ютерних мереж пунктів управління ЗС України	235
146.	**Татарінов А.С., Масесов М.О.** Підвищення пропускної спроможності транспортних мереж, побудованих на обладнанні стандарту IEEE 802.11 шляхом вдосконалення протоколу доступу на мас рівні	236
147.	**Троценко О.Я., Середенко М.М.** Підготовка курсантів вищих військових навчальних закладів до виконання бойових завдань в екстремальних умовах	240
148.	**Турпітько Б.М., Тетерятник І.В.** Автоматизоване робоче місце посадової особи служби ракетно-артилерійського озброєння	242
149.	**Фесьоха Н.О., Гелета Д.Р.** Програмний модуль обліку особового складу ввнз на основі чат-боту	243
150.	**Філіпов В.В., Денгін О.Г., Мотрич А.В.** Перспективи удосконалення засобів проводового та волоконно-оптичного зв'язку в механізованому батальйоні	244
151.	**Фриз С.П., Кальватинський О.В., Авсієвич Р.О.** Використання космічних апаратів типу „CUBESAT" у складі космічних систем подвійного призначення	246
152.	**Хлапонін Ю.І., Мазулевский О. Є., Хлапонін Д.Ю.** Функціональна та кібербезпека об'єктів критичних систем військового призначення	247
153.	**Хорошко В.О., Калантаєвська С.В., Макарчук О.М.** Метод корекції зображення з БПЛА при наявності шумів та завад	248
154.	**Хусаінов П.В.** Виявлення несанкціонованої модифікації параметрів програмно-апаратних засобів обчислювальної системи на основі ідентифікації елементів мікропрограмного управління	250

155.	**Ципук О.Р.** Програмний модуль автоматизації організації навчального процесу на основі чат-Боту Telegram	251
156.	**Цімура Ю.В., Хоменко П.В., Чуб К.С.** Особливості сумісної роботи УКХ радіозасобів виробництва Mototrbo та Aselsan	252
157.	**Чабаненко П.П., Розгонаєв С.М., Бігун Н.С.** Навчання операторів інформаційно-комунікаційних управляючих систем	253
158.	**Чевардін В.Є., Пономарьов О.А., Штобза Д.В.** Нові параметри еліптичних кривих для криптографічних додатків	254
159.	**Чередніков С. О.** Тенденції розвитку засобів зв'язку та автоматизації на прикладі застосування гібридних (IP-TDM) систем диспетчерського та конференц-зв'язку та автоматизованих систем радіорелейного зв'язку	256
160.	**Черноног О.О., Жовтун А.А., Терещенко Т.П., Козубцов І.М.** Вибір автомобільної платформи високої прохідності для підрозділів кібернетичної безпеки Збройних сил	258
161.	**Черноног О.О., Куцаєв В.В., Козубцова Л.М., Козубцов І.М.** Поняття терміну глобального колапсу інформаційно-телекомунікаційних систем	259
162.	**Чумак В.К., Шишацький А.В., Борисов О.В.** Методика управління параметрами багатоантенних систем із шумоподібними сигналами	260
163.	**Шаповалов О.В.** Методи формування ознак при поведінковому аналізі трафіка конвергентних мереж	261
164.	**Швець Ю.О., Троцько О.О.** АСУ технологічим процесом Scada-system в застосуванні інтелектуалізації проектування технологічного процесу підприємств Міністерства оборони України	262
165.	**Шейгас В. В.** Способи виявлення та протидії безпілотним літальним апаратам у Збройних силах України	263
166.	**Шинкарук О. М., Лисий М. І., Бабій Ю. О.** Розпізнавання рухомого об'єкту та оцінка параметрів сигналу від сейсмічного засобу охорони кордону	265
167.	**Шишацький А.В., Сова О.Я.** Використання еволюціонуючих нейро-фаззі систем в задачах інтелектуального оцінювання радіоелектронної обстановки	267
168.	**Шишацький А.В., Остапчук В.М., Олексенко В.П.** Методи оцінки стану каналу зв'язку на основі штучних нейронних мереж, що еволюціонують	269
169.	**Шнукало А.Д., Любарський С.В.** Підвищення ефективності завдань з планування організації зв'язку в автоматизованій системі управління зв'зком	270
170.	**Шолудько В.Г., Андріюк М.С.** Організація супутникового зв'язку в механізованому батальйоні. Перспективи удосконалення засобів супутникового зв'язку	271
171.	**Шпак О.О., Сова О.Я.** Модель автоматизованої системи логування на основі стеку ELK+KAFKA для відслідковування та аналізу подій у мережах	273
172.	**Якорнов Є.А., Цуканов О.Ф.** Алгоритм оцінки параметрів руху безпілотних летальних апаратів	274
173.	**Якорнов Є.А., Цуканов О.Ф.** Алгоритми розподілу різнорідних безпілотних літальних апаратів для нанесення ударів по об'єктам, які чинять опір	276
174.	**Яровий В.С., Радзівілов Г.Д., Гладких В.М.** Проблеми розвитку системи технічного обслуговування та ремонту засобів зв'язку і автоматизації Збройних сил України	278
175.	**Ярошенко Р.Р., Нерознак Є.І.** Розподілена система централізованого збору, зберігання та обробки даних на основі Nextcloud	280
176.	**Ясинецький В.П., Кас'яненко М.В., Опенько П.В., Штаненко С.С**. Рекомендації щодо застосування GSM модуля для збільшення дальності повітряного радіозв'язку	281

Contents

1.	**H.Avdieienko, N.Denysenko** Wireless communication system based on use of uwb transceivers DWM1000	15
2.	**O. Alexandrov, S. Simonov** Issues of information and technical connection modern complex of automation means with movable objects for control using radio stations of the VHF range	17
3.	**V. Ananin, O. Saienko** Paradigmatic fundamentals formation of a modern military personnel	18
4.	**O. Ananin, O. Sayenko** RFID devices used in modern passport documents	20
5.	**Уи. Angelov, O.Simonenko** Model of fault-tolerant object storage using CEPH technology	21
6.	**A.Arsenovich, D.Ivashchuk, N.Timoshishin** Perspectives on the use of Morse code in communications forces	22
7.	**S.Artyuk, E.Lazorenko** Security analysis of monitoring and surveillance systems of the Armed Forces of Ukraine	23
8.	**A.Babarika, I.Katerynchuk, S.Tabensky** Application of image recognition algorithms based on neural network technologies	24
9.	**V.Bakanov, V.Chevardin** Prospects for development of information networks of the Armed Forces of Ukraine	26
10.	**O.Baranovsky, A.Zhilin, I.Novitsky** Methods for detecting malicious traffic based on behavioral analysis	27
11.	**O.Baranovsky, A.Zhilin, O.Pilipenko** Fake base station detection method based on analysis of station re-selection parameters and radio-electronic environment	28
12.	**O.Bardin, O.Nemchenko** Perspectives on the use of „Shock core" ammunition for self-defense of ground combat platforms	29
13.	**D.Basanets, O.Kirgan** Software for the analysis of statistics on the accounting of material resources in the apartment and service	32
14.	S**.Beznosenko, B.Dobropas, O.White, Z.Ponomarenko** Ways to improve the troop metro system	33
15.	**A.Bessalov, L.Kovalchuk, N.Kuchinskaya, O.Telizhenko** The substantiation of the cryptographic stability of the key encapsulation algorithm proposed for standardization	36
16.	**O.Bilash, T.Hlova, M.Sorokatyy** Improvement of training military specialists on the basis of intensification of practical employment	37
17.	**O.Bilash, T.Glova, M.Sorokaty** Improvement in training of military specialists on the basis of of practical training intensification	38
18.	**P.Biryukov** Experience of training US military professionals in a synthetic virtual environment	40
19.	**V.Bovda** Petri-object model for transportation of material in military units	42
20.	**E.Bovda** Combat Deployment Deployment Based on Joint Operations Experience	43
21.	**A. Boyko, A. Bualo, V.Pylypchuk** Methodology of android operation system on mobile devices for prevention of statistical information transmission	45
22.	**L.Bondarenko, O.Bondarenko, K.Buzayeva, V.Rudenko** Telecommunication Infrastructure Management of the Armed Forces of Ukraine: Status, Objectives, Approaches and Prospects	46
23.	**I.Borisov, D.Berezansky, D.Petrova** Substantiation and summary of a mimo system for processing signals under the influence of intentional interference	48
24.	**R.Bruyaka, Ya.Grohololsky** Option to upgrade the telecommunication kit type-1	50
25.	**M. Buhaiov, R. Kaletynets** Method of radio transmission parameters determination with fast frequency hopping spread spectrum and frequency manipulation	51
26.	**S.Vasylenko** Coding the marker of synchronization in subsystem of entry into synchronism of radio communication system with frequency hopping spread spectrum technology	53
27.	**V. Vasylyshyn, V. Lyutov** Estimation of transfer characteristic of the communication channel in OFDM systems using SSA method	54
28.	**O.Vlasenko, V.Gorgulenko, V.Andrusenko** Application of NOSQL database management systems in the creation of information systems of the Armed Forces	55
29.	**O.Vlasenko, V.Gorgulenko** Application of NOSQL database management systems for upgrading military information systems	56
30.	**M.Voytovych, K.Lishchynska, R.Pak, A.Senyk** Implementation of distance learning for improving the training of military professionals	57
31.	**A.Golubyatnikov, A.Blazova** Fireworks - the basis of network security	58
32.	**V.Gorbenko, M.Martoshenko** Mainly information system with discipline "system software and computer architecture"	60
33.	**V.Gorbenko, O.Sachok** Subsystem of accounting of computer facilities of educational and laboratory complex of department of high school	61
34.	**I.Gorbenko, E.Kharlamov** Special-purpose monitoring system for web-based information technology	62

35.	**V. Horlynskyy, V. Ananin** Improvement in Military personnel Training: a safety aspect	63
36.	**O.Grachev** L3HARRIS - results and new perspectives	64
37.	**O.Hrebenuk, A.Martynchuk, M.Rogovets , O.Hrebenuk** Spatially polarized signals processing influenced of barriers in radiomonitoring devices with dual polarization antennas	66
38.	**P.Gurjii, I.Kovalenko, I.Gurjii** Functionality analysis of specialized software for keeping registers of electronic means and determination of their electromagnetic compatibility	67
39.	**T.Gursky** Increasing the noise immunity of VHF air repeaters in the context of intentional noise interference	69
40.	**S.Davidenko, B. Boychuk** Telecommunication networks convergence principles	77
41.	**A.Davidov** Determining rate efficacy of radio-light support tactical aviation in airfield zone	78
42.	**B. Demidov, O. Kapranov, Yu. Kucherenko, A. Tkachov** Automated control systems of interspecific grouping as an integral part of his ability	79
43.	**A.Dneprovska, P.Zhuk** Development of the multifunctional automated system of EW of the Armed Forces of Ukraine prospects	81
44.	**O.Draglyuk, V.Shkorupsky V.Revutsky** Resource-Planning Decision Support Software Opportunity and Usage	83
45.	**M.Dukhanov** Latest L3HARRIS communications technology and software	87
46.	**I.Dyukov** Detection and formation algorithm of radio interference to radio communications with broadband signals	88
47.	**V. Yerokhin, M. Irkha** Methods and results of analysis for demodulator noise fm-signal with compensation of a likely interference	89
48.	**R.Zhivotovsky** Methodological bases for radio frequency resource management of special purpose radio communication systems	91
49.	**O. Zhuk** The method of channel signal formation in OFDM systems	92
50.	**Y.Zhuravskyy, A.Shishatsky** Methodological bases of estimation of radio-electronic situation on the basis of fuzzy clustering of time series	93
51.	**M.Zavyalov, V.Grinkov** Organization of network intelligence by means of Internet services	94
52.	**O.Zaitsev** The methodical approach to determining the advantages of the hypotheses presented in the view of competitive interval evaluations	95
53.	**V. Zalevsky** Closing of telecommunication channels to communication with drones	96
54.	**A.Zarubenko, V.Polivoda, A.Martyniuk** State and prospects of radio communication usag in the armed forces of Ukraine	97
55.	**Y.Zdorenko, D.Kuznetsov** Big data processing methods in military medical information systems	98
56.	**Y.Zdorenko, O.Lavrut, D.Dygan** A method of analytic processing of computer network traffic data	99
57.	**S.Zrol, O.Trotsko** Analysis of cisco ise security network access	100
58.	**M.Ivchenko, V.Tkach, V.Musienko, O.Shugaliy, R.Ochichenko** An analysis of existing problems with the provision of state-of-the-art communications and automation facilities	101
59.	**D. Ischenko, V. Kyryliuk** Control of troops (forces) disruption model for the predicted complex application enemy fire weapons and electronic jamming	103
60.	**D.Kamak, O.Rudenko, O.Skiba, I.Domanov** Problems in the development of modern hardware communications	105
61.	**D.Kamak, O.Rudenko, O.Skiba, S.Trotik** Application of Special Information and Telecommunication Means to Support Anti-Terrorist Action on Military Objects	106
62.	**I.Karasenko** The Delta Integration Platform as a new kind of information gathering	108
63.	**L. Kizlo, S. Radzikovskyi, O. Zhuk** Modern approaches to improving training process for military specialists	109
64.	**D. Koval, M. Yaremchuk** Trends in electronics development on the example of the microcontroller controlled frequency synthesizer	111
65.	**V.Kolesnik** The method of multifactor identification of users at military sites	112
66.	**D.Koltovskov** Methods of intelligence and protected channels construction for control of tactical UAVs	113
67.	**V.Konovets** Some aspects of the security of information interaction with sensors in the surveillance system of the surface	115
68.	**A.Korkin, V.Didik, V.Symonenkov** Construction of effective information-control systems in the composition of terrestrial robotic complexes in support of network-centric scenarios of operations	116
69.	**V.Kotiubin, O.Romanov** Algorithm for searching the period of digital sequence based on independent comparison and synchronous accumulation	118
70.	**V. Krotov** Analysis of traffic modeling approaches in terms of compliance with tactical management networks	120
71.	**D. Koval, M. Yaremchuk** A trend of electronics development on the example of the microcontroller controlled frequency synthesizer	121

72.	**O.Kuvshinov, I.Zotova, S.Bogoly** Synthesis of high-efficiency turbo-code signal-code structures	122
73.	**V.Kuzavkov, A.Zarubenko** Method of synthesis of digital corrective device of system of automatic control of position of platform of antenna field of mobile base station	123
74.	**O.Kuznetsov, D.Kovalchuk., A.Dyachenko, V. Safonenko, S.Datsenko** Performanc e of hashing algorithms suitable for use in blockchain networks	124
75.	**S. Leontovych, M. Zakalad, V. Beliachenko** Substantiation of criteria for evaluation of applicants for the role of Software Development Contractors for the needs of the Armed Forces of Ukraine	126
76.	**O.Lysenko, V.Yavisya, V.Petrova** Choosing a method for obtaining control information by a nanosatellite motion stabilization system	129
77.	**O.Lysenko, V.Yavisya, D.Yavisia** Orientation system for telecommunication nanosatellites	131
78.	**S.Liventsev, V.Pavlov, Yu. Vasilyuk, G.Lyashenko** Algorithm of blind processing of estimation of scalar and vector channels at decoding of turbocodes in channels with structural impediments	133
79.	**K.Lishchynska, M.Sokil, N.Sokulska, A.Senyk** Organization of information systems based on specialized mathematical methods	134
80.	**A.Mazulevsky, A.Sachchenko, V.Tolstikh** Network-level IPS capability analysis	135
81.	**I.Makarchuk, S.Skiba** Information system for automation of work processes of scientific and technical library of higher education institutions within Koch	136
82.	**V.Makarchuk, V.Martyniuk, S.Palamarchuk, A.Karpenko** Analysis of the communications planning process in the Armed Forces of Ukraine and NATO	137
83.	**O.Makoveychuk, I.Ruban, G.Khudov** A new type of augmented reality tokens	139
84.	**O.Maryliv, S.Mieshkov** Calculation of time intervals for the use of UAVs equipped with thermal imaging systems	140
85.	**O. Marfin, O. Symonenko** Analysis of application frameworks for web application development	141
86.	**M.Masesov** Prospects for the development of military transport telecommunications networks	142
87.	**A.Mashkin** Algorithm for Structural Adaptation of Complexes of Mathematical Models of Operations (Combat Actions) under Time Limitations for Obtaining Calculation Results	143
88.	**S.Mikus, O.Voitko, O.Mazulevsky** Key Guidelines for Combating Hybrid Threats in Cyberspace (Across Cyberspace) by NATO's Ministry of Defense and Armed Forces	144
89.	**O. Myronchuk, O. Shpylka** Modeling of communication channels with predefined correlation properties	146
90.	**V. Mykhalevych** An approach to modeling of information and telecommunication supply of C4 in task forces operation	148
91.	**I.Mikhalchuk, V.Statsenko** Adaptive system of automated testing (testing) of cadets' knowledge	149
92.	**D. Mogylevych, I. Kononova** The analysis methods improving reliability software of the control systems for military and weapons	150
93.	**D. Mogylevych, I. Kononova** Technique of organization for maintenance the complex technical system	152
94.	**V.Moldovan, M.Kinah** Information security in modern smartphones with operation system android	153
95.	**A.Moroz, E. Neroznak** Implementation of remote administration of network and server equipment	154
96.	**O. Nahorniuk, Yu. Kolos** Influence of composing constructive solutions and errors in the manufacturing of the wideband horn antenna on its technical characteristics	155
97.	**I. Nazarenko, O. Trotsko** Model of network incident response system based on ELK software stack	156
98.	**E.Neroznak, A.Kravchenko, O.Sova** Analysis of methodologies, architectural solutions and tools for developing information systems and networks	157
99.	**M.Nesterenko, A.Bayura** Software module for adaptive model building for 3D printing using FDM technology	162
100.	**M.Nesterenko, V.Bogutsky** Virtual training complex "Telecommunication set TIP-1" based on UNITY3D software environment	163
101.	**M.Nesterenko, B.Tkachenko** Software module for configuring and managing a segment of the virtual network SDN	165
102.	**O.Nesterov , I.Zinchenko , M.Zinchenko** Method of assessing the speed capacity of the special purpose communication system based on typical dendrograms with typical models of communication	166
103.	**O .Ovsiannikov, O.Havruliuk, Y.Chernish** Implementation of the service "Identification and Authentication in exchange" in international standards	167
104.	**V.Ovsyannikov, N.Palamarchuk, S.Palamarchuk, O.Cherednichenko** Approaches to the formation of requirements for protection of information against unauthorized access during the development of software for automated systems	168
105.	**M.Oksyonenko, S.Yakovlev** Methods for detecting hidden facelift-like transformations	170
106.	**V.Olshansky, I.Kuhar, Yu.Yegorov** Automated control system "Nettle"	171

107.	**O.Ostapuk, N.Grishina, O.Karaban, T.Poberezhets** Options for resolving information security in a multi-service communications network	172
108.	**V.Orlov, V.Symonenkov** Development of passive systems of sound location of uav is in terms of terrorist threats	175
109.	**K. Pavlenko** Prospects for development of engineering ammunities in the conditions of the hybrid war	176
110.	**O.Pavlenko** Directions of introduction of simulation modeling systems while the training military specialists	177
111.	**V. Pashchetnyk, O. Pashchetnyk** Interdisciplinary intergration of knowledge in at higher military institution	179
112.	**O. Pashchetnyk, V. Zhuvchyk, L. Polishchyk** Development of the ontological system of decision-making support for the commanders of tactical control level of the armed forces of Ukraine	180
113.	**Y. Pilipchuk, D.Petrov, A.Ostapuk, A.Getman** Current trends of information systems development in the Armed Forces of Ukraine	181
114.	**V.Pylypchuk** Detection method of movable maritime objects on digital images of iconics instruments	185
115.	**I.Pavtoraiko, V.Lakhno** Detection of anomalies using an outlier approach	186
116.	**L. Pogrebniak, I. Kononova** Analysis of effectiveness of protective and spatial coding in double-selective channels of military radio communication systems	188
117.	**V.Podlipaiev, I.Khizhnyak** Analysis of modern geoinformation systems of transdisciplinary use of unless-structured data	189
118.	**O.Pokotilyuk, I.Stotsky** Software module for calculating the possible consequences of a nuclear explosion	191
119.	**A. Polisky** Filtration of evaluations of condition vector elements provided that targets motion is uniform and straightforward.	192
120.	**M.Poluyanenko, O.Onikiychuk, E.Demenko, M.Goncharov, N.Pisarenko** Double Cost Probability in Blockchain Systems Based on „Independent Players Model"	193
121.	**V.Chernyaev, A.Pomin, L.Kolodiychuk** Radio-relay component of mobile digital throposphere-radio-relay station	185
122.	**Yu. Pushkaryov, V.Revenko** Synthesis method of automatic tracking systems of high precision control	197
123.	**S.Rybka, A.Korolev, I.Varava** Software for designing digital filters by frequency sampling	198
124.	**Y. Ryzhov, L. Sakovych** Method of time distribution for repair of radio electronic means with multiple defects	199
125.	**O. Ryhalsky, S. Natalchuk** Assessment of the impact of parameters of the communication channel on the quality of information transmission in the mobile systems of the gsm standard	200
126.	**I.Romanenko** Analysis of tasks and methods of evaluation and choice of alternative solutions	201
127.	**V.Romanyuk** Algorithm for positioning telecomunication aeroplatforms for increasing throughput flying networks	203
128.	**V.Rudenko, L.Bondarenko, K.Buzayeva, O.Ostapuk** Prospects for the development of tropospheric communications in the Armed Forces of Ukraine	208
129.	**M.Rudenko, O.Simonenko** Model of organization of the kibana visualization system in special purpose networks	210
130.	**V.Rutsky, O.Trotsko** Analysis of remote automated management of network infrastructure	211
131.	I**.Samoilov, G.Zastelo** The use of artificial intelligence to extract fuzzy relationships from experimental data	212
132.	**A.Semenov, O.Trotsko** Analysis of factors affecting the specific data transmission network	213
133.	**P.Serdyuk, V.Slyusar** Augmented Reality Technologies - Current State and Perspectives	214
134.	**O. Sydorchuk, D. Klimenko, V.Dvorsky** Small hole roller radiator of mirror antenna systems of radio-technical station stations	215
135.	**O. Sydorchuk, R. Levonets** Research of electromagnetic field for design of mirror antenna systems of radiation or radiotechnical station stations	216
136.	**O.Simonenko, A.Bilan, O.Zhuk** Cyberterrorism in the Context of Building State Cybernetic Protection System	217
137.	**V.Slusar** The concept of vehicle architecture as network of networks	218
138.	**E.Slyusar, E.Redzyuk** The program module of analytical data processing for success of training groups	220
139.	**N. Sokulska, B. Sokil, R. Kovalchuk, V.Kmin** Distance learning as one of the ways for improving military specialists training	221
140.	**V. Solodovnick, T. Vysotska, R. Osmanov** Bit Error Rate Performance Evaluation of Space Coding Methods with Dual-Mode Index Modulation Aided OFDM	223

141.	**M.Sorokatyy, O.Petruchenko, O.Bilash** Specifity of teaching higher mathematics in Higher Military Education Institute	225
142.	**E.Stepanenko** Evaluation of the effectiveness of management topology techniques FANET	227
143.	**D.Stupak** Methods for assessing the effectiveness of the functioning of the quality assurance system of higher military education	231
144.	**B.Sus, Ya.Grohololsky** The physical meaning of the concept of „displacement current"	233
145.	**V.Tarara E.Neroznak** Implementation of remote access to computer networks of Ukraine armed forces management points	235
146.	**A.Tatarinov, M.Masesov** Increase the capacity of transport networks built on IEEE 802.11 equipment by improving the mass access protocol	236
147.	**O. Trotsenko, M. Seredenko** Training kadets of military academies for carrying out combat tasks in extreme conditions	240
148.	**B.Turpitko, I.Teteryatnik** Automated workplace for a missile and artillery officer	242
149.	**N.Fezokha, D.Geleta** Software module for accounting of personnel on the basis of chat bot	243
150.	**V.Filipov, O.Dengin, A.Motrych** Perspectives on Improvement of Wired and Fiber Optic Communication in a Mechanized Battalion	244
151.	**S. Fryz, O. Kalvatynsky , R. Avsievich** CubeSat satellites application in the dual purpose space systems	246
152.	**Yu.Khlaponin, O.Mazulevsky, D.Khlaponin** Functional and Cyber Security of Criti cal Military Objects	247
153.	**V.Khoroshko, S.Kalantayevskaya, O.Makarchuk** UAV image correction method in the presence of noise and interference	248
154.	**P.Husainov** Detection of unauthorized modification of the parameters of software and hardware of the computer system based on the identification of the firmware controls	250
155.	**O.Tsipuk** Software module for automation of organization of educational process on the basis of Telegram chat-bot	251
156.	**Y.Timura, P.Khomenko, K.Chub** Features Of Joint Work Of Vhf Radio Products Manufactured By Mototrbo And Aselsan	252
157.	**P.Chabanenko, S.Rozgonaev, N.Bihun** Operators training of information and communication management systems	253
158.	**V.Chevardin, O.Ponomarev, D.Shtobza** New Elliptic Curve Options for Cryptographic Applications	254
159.	S**.Cherednikov** Trends in Communication and Automation Development Using the Case of Hybrid (IP-TDM) Dispatch and Conference Communication Systems and Automated Relay Systems	256
160.	**O.Chernogog, A.Zhovtun, T.Tereshchenko, I.Kozubtsov** Choosing a High-Speed Car Platform for the Armed Forces Cyber Security	258
161.	**O.Chernogog, V.Kutsayev, L.Kozubtsova, I.Kozubtsov** The concept of the term global collapse of information and telecommunication systems	259
162.	**V.Chumak A.Shishatsky, O.Borisov** Methods of parameter management of many antenna systems with noise signals	260
163.	**O.Shapovalov** Methods of trait formation in behavioral analysis of convergent network traffic	261
164.	**Y.Shvets, O.Trotsko** ACS technological process Scada-system in the application of intellectualization of technological process design of enterprises of the Ministry of Defense of Ukraine	262
165.	**V. Sheihas** Detection and response to free airplanes in the armed forces of Ukraine	263
166.	**O.Shynkaruk, M.Lysy, Y.Babiy** Moving object recognition and estimation of signal parameters from seismic border guard	265
167.	**A.Shishatsky, O Owl** The use of evolving neuro-phase systems in the problems of intellectual evaluation of the radio-electronic environment	267
168.	**A.Shishatsky, V.Ostapchuk, V.Oleksenko** Methods for assessing the status of a communication channel based on evolving artificial neural networks	269
169.	**A.Shnukalo, S.Lyubarsky** Improving the effectiveness of telecommunication scheduling tasks in an automated communications management system	270
170.	**V.Sholudko, M.Andriyuk** Satellite communication in a mechanized battalion. prospects for improving satellite communications	271
171.	**O.Shpak, O.Sova** Model of automated logging system based on ELK + KAFKA stack for event tracking and analysis in networks	273
172.	**E.Yakornov, O.Tsukanov** An algorithm for estimating motion parameters unmanned aerial vehicles	274
173.	**E.Yakornov, O.Tsukanov** Algorithms of distribution of heterogeneous unmanned aerial vehicles for striking objects that resist	276

174.	**V.Yarovyi, H.Radzivilov** Problems of development of maintenance system of communication and automation equipments of the armed forces of Ukraine	278
175.	**R.Yaroshenko, E.Neroznak** Distributed centralized collection, storage and processing data based on nextcloud	280
176.	**V.Yasinetskiy, M.Kasyanenko, P.Openko, S.Stanenko** Recommendations for using the GSM module to increase the range of air radio	281

Авдєєнко Г.Л. (ІТСНТУУ „КПІ”)
Денисенко Н.І. (ІТС НТУУ „КПІ”)

БЕЗПРОВОДОВА СИСТЕМА ЗВ’ЯЗКУ НА БАЗІ ВИКОРИСТАННЯ UWB ТРАНСИВЕРІВ DWM1000

Актуальність. У зв’язку з удосконаленням методів формування, обробки та передачі повідомлень за допомогою технічних засобів телекомунікацій, одним з перспективних напрямків розвитку галузі телекомунікацій є використання надширокосмугових сигналів (далі – UWB). Тому задача технічної реалізації систем зв’язку з використанням наявних на ринку трансиверів UWB сигналів є актуальною та своєчасною.

Постановка задачі. На даний момент часу діапазон частот, що виділений для реалізації систем зв’язку на базі UWB сигналів обмежений смугою частот 3.1-10.6 ГГц, при чому максимальна спектральна цільність потужності випромінювання в цій смузі для забезпечення електромагнітної сумісності з радіоелектронними засобами інших радіосистем не повинна перевищувати -43дБмВт/МГц. Таке мале значення спектральної щільності обмежує радіус дії систем зв’язку з використанням UWB сигналів відстанню, яка не перевищує десятків – сотень метрів.

Мета. Розглянути варіант технічної реалізації системи зв’язку типу „точка-точка” (далі – „PtP”) на базі UWB трансиверів DWM1000.

Основні положення. Безпроводова система зв’язку на базі UWB сигналів має низку переваг:

– відносно невелика складність технічної реалізації передавачів та приймачів;

– висока безпека передачі радіосигналу (низька вірогідність виявлення та перехвату, детектування сигналів);

– електромагнітна сумісність із вузькосмуговими системами бездротового зв’язку;

– стійкість до впливу завади при поширенні багатопроменевого тракту та навмисних чи ненавмисних перешкод;

– висока роздільна здатність сигналу в часовій області, обумовлена його малою тривалістю (менше 1нс);

– можливість повнодуплексного режиму роботи в одній смузі частот;

– невеликі габарити приймально-передавального обладнання;

– висока швидкість передачі даних (сотні Мбіт/с).

На даний момент часу, в світі виробниками UWB трансиверів є такі компанії, як Nanjing Wo Xu Wireless Co., Decawave Ltd., Time Domain Inc., і т.д.

Розглянемо структурну схему дуплексної системи зв’язку типу „PtP”, до складу якої входять персональні комп’ютери(ПК), мікроконтролери(МК), трансивери UWB DWM1000, яка у зображено на рис.1.

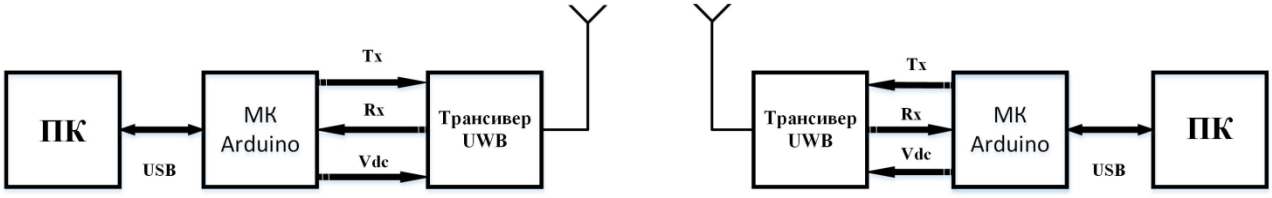
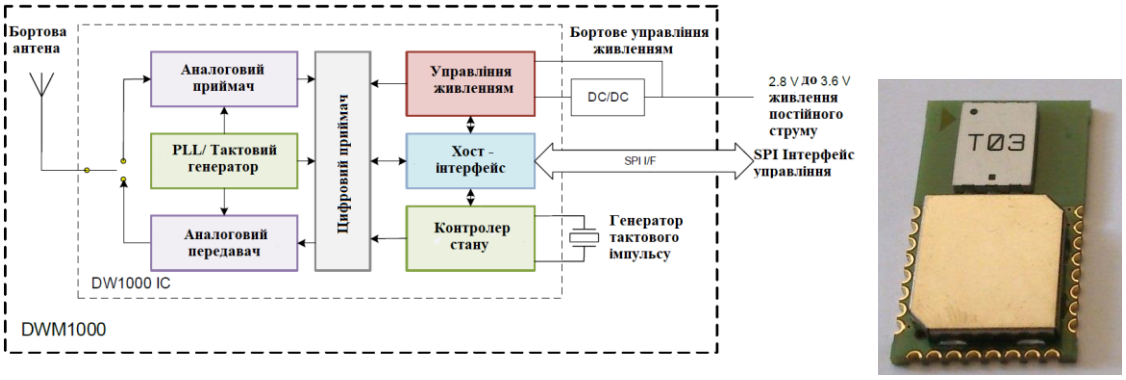


Рис.1 Структурна схема дуплексної системи зв’язку типу „PtP”

В даній роботі розглянуто трансивер DWM1000, який виготовляє компанія DecaWave, що відповідає специфікації стандарту IEEE 802.15.4-2011. Трансивер DWM1000 оптимізований для застосувань у системах локального позиціонування в реальному часі та бездротових сенсорних мережах, включаючи мережу IoT, сільське господарство, управління будівництвом, охорону здоров’я, безпеку, логістику та ряд інших. Структурна схема трансиверу представлена на рис.2 (а), а його фотографія на рис.2 (б).



а) б)

Рис.2 UWB трансивер DWM1000

Відповідно до рис.2(а) трансивер складається з UWB антени, інтегральної мікросхеми DWM1000, генератору тактового сигналу, вузла живлення постійної напруги DC/DC та інтерфейсу управління SPI.

Даний трансивер дозволяє реалізувати наступні функції:

– визначення місця положення об'єктів в режимі реального часу (RTLS) з точністю до 10 см у приміщенні;

– реалізує зв’язок в різних режимах роботи на швидкостях передачі 110 кбіт/с, 850 кбіт/с і 6,8 Мбіт/с;

– дальність зв’язку до 300 м завдяки використання когерентної техніки прийому ;

низьке споживання енергії дозволяє працювати з акумуляторами тривалий час:

– режим передачі від 31 мА;

– режим прийому від 64 мА;

– режим таймеру 2 мкА;

– невеликий фізичний розмір дозволяє реалізувати економічно ефективні рішення в RTLS та WSN;

– вбудована антена забезпечує просту технічну реалізацію продукту;

– підтримуються 4 смуги частот в діапазоні від 3,5 до 6,5 ГГц;

– спектральна щільність потужності випромінювання передавача від -35 дБм/МГц до -62 дБм/МГц;

– довжина преамбули фрейму від 64 мкс до 4 мс;

– підтримує розміри пакетів до 1023 байт;

– модуляція: BPM з BPSK;

– вбудована перевірка FEC та CRC;

– стандартний інтерфейс SPI для хоста (20 МГц);

– сумісний з багатьма видами мікроконтролерів;

– напруга живлення постійного струму від 2,8 В до 3,6 В;

– технології доступу до середовища передачі:

– FDMA: 4 канали;

– CDMA: 2 різні коди / на канал;

– підтримує вимірювання дальності до об’єкту в режимі ToF та в режимі TDOA;

– температурний діапазон від -30 °C до + 85 °C;

– габаритні розміри 23 мм х 13 мм х 2,9 мм;

– 24-контактний пакет.

Висновок. Таким чином, розглянутий UWB трансивер завдяки своїм технічним характеристикам може бути використаним для реалізації передачі даних на відносно великих швидкостях. Проста технічна реалізація та економічність цього приладу дозволяє реалізувати дану систему в різних галузях людської діяльності.

к.т.н. Александров О.В. (ХНУПС)
Сімонов С.І. (ХНУПС)

ПРОБЛЕМНІ ПИТАННЯ ІНФОРМАЦІЙНО-ТЕХНІЧНОГО СПРЯЖЕННЯ СУЧАСНИХ КОМПЛЕКСІВ ЗАСОБІВ АВТОМАТИЗАЦІЇ З РУХОМИМИ ОБ'ЄКТАМИ УПРАВЛІННЯ ЗА ДОПОМОГОЮ РАДІОСТАНЦІЙ УКХ-ДІАПАЗОНУ

Системна інтеграція різноманітних комплексів засобів автоматизації (КЗА) в процесі управління військами видів Збройних сил (ЗС) України дозволяє більш ефективно організувати взаємодію з'єднань, частин родів військ та спеціальних військ, сил та засобів Повітряних Сил, інших видів ЗС у ході підготовки та ведення бойових дій.

Одним із завдань забезпечення інформаційної взаємодії вказаних КЗА з рухомими об'єктами управління є організація середовища передачі інформації з використанням цифрових перешкодозахищених засобів короткохвильового (КХ) та ультракороткохвильового (УКХ) радіозв'язку.

Сучасні засоби КХ та УКХ радіозв'язку (радіостанції виробництва Harris та Aselsan), що надходять на озброєння пунктів управління мобільних частин та підрозділів ЗС України, відповідають сучасним вимогам щодо скритності управління за рахунок можливості використання режиму псевдовипадкової перебудови робочої частоти радіостанції та можливостей щодо криптозахисту інформації (використанням алгоритмів блочного шифрування AES з ключем до 256 біт). Але під час вирішення завдань інформаційно-технічного спряження (ІТС) КЗА з рухомими об'єктами управління з використанням цифрових УКХ-радіостанцій виникає ряд проблемних питань, до основних з яких слід віднести такі.

1. Дальність передачі інформації на радіочастотах діапазону 30-512 МГц суттєво знижується при використанні УКХ-радіостанцій в умовах пересіченого рельєфу місцевості. При цьому необхідно враховувати, що потужність передатчика таких радіостанцій нелінійна по відношенню до спектру частот. Так, радіостанції Harris із заявленою потужністю передатчика 50 Вт забезпечують її в діапазоні частот 30-108 МГц, а в діапазоні частот 108-512 МГц лише 20 Вт.

2. Обмежена кількість абонентів, що підключаються до мережі цифрового радіозв'язку в режимі ANW2, що накладає обмеження до кількісного складу угруповання, що здійснює обмін даними в рамках однієї радіомережі. Так у радіомережі створеної на базі радіостанцій тактичної ланки управління типу Harris RF-7850M кількість абонентів не перевищує 10, при цьому корисна пропускна спроможність каналів зв'язку не перевищує 57 Кбіт/с, що в розрізі сучасних вимог до швидкості обміну даними в тактичній ланці управління є недостатнім.

3. Організація ІТС сучасних КЗА з наземними рухомими об'єктами управління старого парку (наприклад, ЗРК С-300ПС (ПТ)), з урахуванням вимог часової синхронізації, можлива лише в режимі „точка-точка" мережі MACA2, що викликає апаратну надмірність радіостанцій з боку органу управління.

4. Організація ІТС з літаками винищувальної авіації потребує модернізації їх підсистеми зв'язку. Для підключення літака до цифрової радіомережі необхідна модернізація антенофідерних пристроїв його носової та хвостової частини, а також встановлення відповідного приймача. При цьому радіостанція (приймач) повинна забезпечувати можливість приймання даних лише в режимі радіомовчання (підтримку такого режиму забезпечують радіостанції Harris (режим MACA2), на відміну від яких радіостанції Aselsan у мережах NBNR, WBNR здійснюють постійний обмін службовими пакетами даних).

Для вирішення зазначених проблемних питань необхідно здійснити доопрацювання спеціального програмного забезпечення вказаних радіостанцій. Запропоновані шляхи вирішення зазначених проблемних питань. Впровадження запропонованих рекомендацій створить умови для підвищення ефективності інформаційної взаємодії між КЗА та рухомими об'єктами управління у ході підготовки та ведення бойових дій.

д.філос.н. Ананьїн В. О. (ВІТІ)
к.т.н. Саєнко О. Г. (ВІТІ)

ПАРАДИГМАЛЬНІ ЗАСАДИ ФОРМУВАННЯ ОСОБИСТОСТІ СУЧАСНОГО ВІЙСЬКОВОГО ФАХІВЦЯ

На сучасному етапі розвитку Збройних сил України вагомої актуальності набуває визначення та розвиток парадигмальних засад, які мають забезпечити створення умов досягнення високого рівня професійного, інтелектуального і духовного розвитку та саморозвитку військових професіоналів.

Проблема формування особистості військового фахівця знайшла певне відображення у наукових дослідженнях В. Абрамова, Е. Афоніна, В. Баранівського, М. Варія, О. Гаврілова, Р. Доор, М. Корольчука, П. Криворучка, Ч. Коттона, О. Самойлова, Є. Мануйлова, М. Нещадима, О. Панфілова, М. Ротаня, Н. Коупленда, В. Хаузера, В. Ягупова та інших вітчизняних та зарубіжних вчених. Сам процес формування особистості військового професіонала постає як механізм дії законів і являє собою спосіб реалізації об'єктивних законів функціонування та розвитку суспільства, збройних сил, взаємозв'язку армії та суспільства.

Аналіз змісту наукових праць дозволяє окреслити коло сучасних пріоритетів, що мають сприяти розв'язанню поставленої проблеми. Об'єктивна необхідність формування особистості військового професіонала в сучасних умовах має загальнолюдську, суспільну, військово-професійну та особистісну обумовленість.

У військово-професійному аспекті формування особистості військовослужбовців детерміновано необхідністю забезпечення їх готовності та здатності до виконання завдань за призначенням. У суспільному аспекті формування особистості військового професіонала детерміновано необхідністю забезпечення безпеки держави у воєнній сфері, виховання військовослужбовців як громадян і патріотів. Вимогами суспільства до політичних, моральних і професійних якостей військовослужбовців фактично визначається основний зміст формування особистості військового професіонала. В індивідуально-особистісному аспекті формування особистості військового професіонала детерміновано необхідністю реалізації військовослужбовцями своїх духовних і фізичних потенцій.

Стрімкий розвиток військового мистецтва, наукової і технологічної бази, засобів збройної боротьби 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.

До основоположних парадигмальних засад формування особистості військового фахівця належить нове розуміння природи людини як центру соціальної реальності, у тому числі освітньої практики, пов'язаної з трансформацією військово-освітнього процесу та його гуманізацією. Важливим є укорінення цих взаємовідносин через визнання їхнього особистісного сенсу для кожного військового професіонала. При цьому мають змінюватись: способи впливу на людину, її взаємодія з природним і соціокультурним середовищем; уявлення про військову освіту та освіту взагалі; ідеали, норми та цінності освіти. Змінюється поняття фундаменталізації, як категорії якості освіти та освіченості особи, де основним сенсом стає забезпечення оптимальних умов для формування та розвитку гнучкого і багатогранного наукового мислення, різних способів сприйняття дійсності, створення внутрішньої потреби до саморозвитку і самоосвіти протягом усієї служби.

У основу нової парадигми формування особистості військового фахівця покладено також методологію полікультурного діалогу, яка зорієнтована на діалог різних ідеологічних, соціальних систем сучасності, на усвідомлення етнокультурної самобутності різних народів.

Особистість військового професіонала постає суб'єктом творчої діалогічної взаємодії людства. Відтак, освітня діяльність, культура, наука спрямовуються на формування світоглядно-творчих орієнтацій, підготовку інтелектуально-розвинених, конкурентоспроможних фахівців міжнародного рівня.

Наступним напрямком підготовки – виступає формування військової людини як гармонійно і всебічно розвиненої, високодуховної, відповідальної особистості, здатної конструктивно й ефективно працювати у екстремальних ситуаціях військової діяльності. Соціальна складова парадигми формування особистості військового фахівця включає відображення аспекту існування військової освіти в широкому соціокультурному середовищі і передбачає дослідження впливу на функціонування військової освіти таких сутнісних чинників як держава, культура, наука, техніка, збройні сили тощо. Освіта як соціальний інститут відповідно реагує на всі зрушення, що відбуваються в суспільстві. За рахунок поширення інформаційно-освітніх технологій змінюється характер усіх сфер соціального життя.

Ціннісна складова парадигми військової освіти включає дослідження духовно-ціннісних аспектів людського виміру військово-освітньої системи та військово-освітньої діяльності й пов'язана з обґрунтуванням визначення ідеалів, норм та пріоритетних цінностей і смислів духовного світу військових професіоналів.

Пізнавальна складова парадигми військової освіти має на меті гносеологічне обґрунтування її предмета та категоріально-понятєвого апарату. Пріоритетним напрямком пізнавальної складової виступає з'ясування того, які науки, дисципліни та інтегративні підходи мають скласти основу для розробки засад сучасної парадигми військової освіти країни.

Особистісна складова парадигми системи підготовки військового фахівця передбачає проектування педагогічного процесу, де реалізуються такі концептуальні засади: основними суб'єктами навчання та виховання є військовослужбовці; основною метою педагогічного процесу є створення умов для активної навчально-пізнавальної діяльності військовослужбовців та розвиток їхніх індивідуальних здібностей. Пріоритетними аспектами у визначенні особистісної складової парадигми виступають нове розуміння людини, її природи як центру всієї соціальної реальності, у тому числі й військово-освітньої царини; формування й розвиток соціально-відповідальної особистості, здатної конструктивно та ефективно вирішувати завдання в проблемних, нестандартних ситуаціях військової діяльності.

Дидактична складова парадигми підготовки військового фахівця трансформує всі попередні компоненти (соціальну, ціннісну, пізнавальну, особистісну) до рівня практичного проектування та втілення військово-освітніх систем нового типу відповідно до світових змін в освітній царині. Дидактична складова компонента включає в себе такі заходи: створення багаторівневої безперервної системи підготовки військових фахівців протягом усієї служби; технологізацію, фундаменталізацію, інформатизацію навчального процесу і трансформації ролі військового керівника в системі суб'єктно-об'єктних відносин навчання.

Обґрунтовані компоненти парадигми військової підготовки 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.

Висновок Стратегія розвитку системи підготовки військового фахівця, яка будується на сучасних парадигмальних засадах, має забезпечити підготовку військовослужбовця з високим рівнім професійного, інтелектуального і духовного розвитку.

к.т.н. Ананьїн О. В. (ГЕКЦ ДПСУ)
к.т.н. Саєнко О. Г (ВІТІ)

RFID-ПРИСТРОЇ, ЯКІ ВИКОРИСТОВУЮТЬСЯ У СУЧАСНИХ ПАСПОРТНИХ ДОКУМЕНТАХ

Відповідно до вимог міжнародних стандартів ICAO Doc 9303, у сучасних паспортних документах, використовується безконтактний електронний носій інформації, який являє собою інтегральну мікросхему з безконтактним інтерфейсом та реалізований на базі RFID-технології (RFID-пристрій).

RFID-пристрій виконує функції: додаткового захисту документу від підроблення; забезпечення автоматизації процедур прикордонного контролю фізичних осіб; додаткового підтвердження автентичності фізичної особи-пред'явника, а також самого документу, який посвідчує особу, відповідно до законодавства України.

У наш час певним недоліком реалізації RFID-технологій є зовнішня антена, яка за розмірами перевершує саму мікросхему у кілька десятків і більше разів. Виготовлення RFID-антен для паспортних документів виконується традиційною технологією – гравіюванням міддю з мідних субстратів. Така антена легко піддається механічним пошкодженням при необережному поводженні з документом. Пошкодження антени унеможливлює встановлення зв'язку із термінальним пристроєм прикордонного контролю та зчитування інформації, що міститься на електронному носії. Через це виникають певні ускладнення із підтвердженням автентичності фізичної особи-пред'явника, самого документу, який посвідчує особу, а також автоматизації процедури прикордонного контролю особи.

Таким чином, дослідження проблем, пов'язаних із удосконаленням способів виконання антен для RFID-пристроїв, які використовуються для захисту паспортних документів залишається актуальним науковим та практичним завданням.

Метою доповіді є викладення удосконаленого способу виконання антен для RFID-пристроїв, які використовуються у сучасних паспортних документах України.

Наразі, найбільш економічним способом виготовлення антен для RFID-пристроїв є друк струмопровідними фарбами (поліграфічний спосіб). Такі фарби вважаються більш рентабельним рішенням. Вартість фарб нижче ніж коштують традиційні технології з використанням металевих субстратів.

Струмопровідні фарби класифікуються, як тверді фарбуючи матеріали для друку флексографським способом. За їх допомогою друкують електронні схеми на різні види полімерних матеріалів та папір. Струмопровідні фарби містять електропровідні матеріали, зокрема срібло. Через високу проводимість срібла, фарби на його основі використовуються у друкованій електроніці.

У сучасних умовах, друкована електроніка являє собою набір друкарських методів, які використовуються для створення електричних пристроїв на підкладках із різних матеріалів. Друкована електроніка вже давно використовується для виготовлення гнучких дисплеїв, смарт-етикеток, анімаційних плакатів тощо.

Полімерні матеріали та папір, які використовуються для виробництва паспортних документів мають важливі властивості, такі як відповідний опір та еластичність.

Наразі, за кордоном досвід виготовлення RFID-антен шляхом використання струмопровідних фарб передбачено реалізувати у Білорусії. Зокрема, впровадження такої технології у паспортних документах Білорусії передбачається у 2020 році.

Висновок. Викладений поліграфічний спосіб щодо удосконалення реалізації антен спроможний вирішити проблему з удосконалення RFID-пристроїв, які використовуються у сучасних паспортних документах. Але, у результаті аналізу сучасних способів реалізації RFID-технологій, дослідження проблем, пов'язаних із використанням для захисту документів RFID-пристроїв з поліграфічним виконанням антен на базі струмопровідних фарб і на далі залишається актуальним науковим та практичним завданням.

Ангелов Ю.С. (ВІТІ)
Симоненко О.А. (ВІТІ)

МОДЕЛЬ ВІДМОВОСТІЙКОГО ОБ'ЄКТНОГО СХОВИЩА ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ *CEPH*

Актуальність цієї теми полягає в тому, що хмарні файлові сховища продовжують набирати популярність, і вимоги до них продовжують рости. Сучасні системи вже не в змозі повністю задовольнити всі ці вимоги без значних витрат ресурсів на підтримку і масштабування цих систем. Під системою я маю на увазі кластер з тим чи іншим рівнем доступу до даних. Для користувача важлива надійність зберігання і висока доступність, щоб файли можна було завжди легко і швидко отримати, а ризик втрати даних наближався до нуля. У свою чергу для постачальників і адміністраторів таких сховищ важлива простота підтримки, масштабованість і низька вартість апаратних і програмних компонентів.

У ЗСУ продовжується розвиток технологій для безпечного зберігання даних та для запобігання їх втрати, адже втрата будь-якої інформації може нести за собою тяжкі наслідки, в тому числі втрата особового складу підрозділів або важливих об'єктів. Вчасне надання даних може відіграти головну роль у військовій сфері, саме тому була розроблена модель відмовостійкого об'єктного сховища за допомогою нової технології, а саме технології *Ceph*.

Модель відмовостійкого об'єктного сховища за допомогою *Ceph* – це кластер вузлів для зберігання та реплікації даних і подальшого запобігання їх втрати. Дана система була розроблена для зниження ризику втрати даних до мінімального рівня, в той самий час зробити функціонування цієї системи максимально автоматизовано і просто для користувачів та адміністратора, у разі необхідності його втручання у систему. За допомогою цієї моделі було створене об'єктне сховище, яке при завантаженні у нього даних, робило реплікації (копії) на інші сервери та при відмові у роботі серверу система не втрачала дані, а створювала відповідну репліку на інший сервер. Система робить репліки до тих пір, поки сервери (жорсткі диски) будуть виходити з ладу і будуть наявні в мережі системи інші сервери, на яких ще не має реплік даних, які були втрачені разом з сервером.

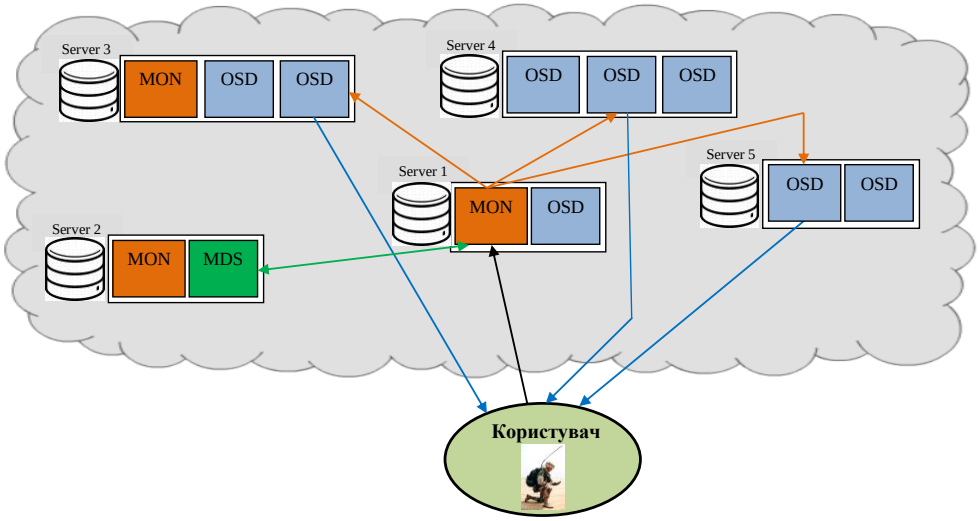


Рис.1 Модель сховища за допомогою технології *Ceph*

Таким чином, запропонована модель може функціонувати як у великих системах ЗСУ, так і у малих, як наприклад на інститут чи його окремі кафедри для зберігання та запобігання втрати важливих дани, документації, навчальних матеріалів тощо. Модель відмовостійкого об'єктного сховища за допомогою технології Ceph дозволить максимально скоротити ризики втрати даних через відмову чи несправність пристоїв зберігання та мінімізувати втручення адміністраторів у систему, тим самим задовольняє вимоги гнучкості, простоти і зручності використання.

Арсенович А.Д. (ВІТІ)
Іващук Д.І. (ВІТІ)
Тимошишин Н.М. (ВІТІ)

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ АЗБУКИ МОРЗЕ У ВІЙСЬКАХ ЗВ'ЯЗКУ

Самюел Фінлі Бриз Морзе народився 27 квітня 1791 р. у родині відомого місцевого проповідника Джедіда Морзе в американському містечку Чарльзтаун. Працюючи над вдосконаленням свого телеграфного апарата Самюел Морзе в 1838 р. винайшов і код – телеграфну абетку. Саме вона була названа на честь цього американського винахідника Семюеля Морзе, який її запропонував.

За одиницю часу приймається тривалість однієї точки. Тривалість тире дорівнює трьом точкам. Пауза між елементами одного знака – одна точка, між знаками в слові – 3 точки, між словами – 7 точок. Принцип кодування абетки Морзе полягає в тому, що букви, які частіше вживаються в англійській мові, кодуються простішими поєднаннями крапок і тире. Це робить освоєння абетки Морзе простіше, а передачі – компактніше.

В абетці Морзе також можна використовувати абревіатури. Ось найпоширеніші серед них: 73 – найкращі побажання, R – вас зрозумів, QRS – передавайте повільніше, GM-привітання, GB – до побачення.

Азбука Морзе свого часу відіграла дуже важливу роль в судноплавстві і авіації, а також широко застосовувалася під час війн. Пілоти повинні були вміти спілкуватися азбукою Морзе. За останні три роки частини і підрозділи зв'язку зазнали певного розвитку, отримали на озброєння новітні цифрові засоби передачі інформації та техніку зв'язку, що надає їм можливості виконувати ними завдання за призначенням. У наш час, як правило, використовують більш сучасні засоби зв'язку, але застосування прийому на слух знаків телеграфної азбуки „Морзе" під час ведення радіообміну все ж таки відбувається, хоч і повільно, в порівнянні з цифровими способами передачі інформації.

Азбуку Морзе застосовують на флоті, в розвідці та в МНС. Вона дуже популярна серед радіоаматорів. „Морзянка", швидше за все, не вмре ніколи, адже це найдоступніший і простий спосіб зв'язку. Приймати сигнал можна на далеких відстанях і в умовах сильних радіоперешкод (це є єдиним способом забезпечення зв'язку), кодувати послання можна вручну, а запис і відтворення відбувається за допомогою найпростіших пристроїв.

Таким чином, азбука Морзе не підведе в надзвичайній ситуації, якщо з ладу вийде більш складне обладнання. Передаватися і прийматися азбука Морзе може з різною швидкістю – це залежить від можливостей і досвіду радистів. Зазвичай середньої кваліфікації радист працює в діапазоні швидкостей 60 – 100 знаків на хвилину. Рекорди за швидкісними прийому-передачі знаходяться в діапазоні швидкостей 220 – 260 знаків за хвилину.

Переваги при застосуванні азбуки Морзе:

– Висока перешкодозахищеність при прийомі на слух в умовах сильних радіоперешкод.

– Можливість кодування вручну.

– Запис і відтворення сигналів найпростішими пристроями.

– Можливість передавання за допомогою світлових сигналів, а також за допомогою жестів (прапорцями).

Недоліки:

– Неекономічність, на передачу одного знака коду потрібно в середньому – 9,5 елементарних посилок.

– Мала придатність для букводрукуючого прийому.

– Низька швидкість телеграфування.

Артюх С.Г. (ВІТІ)
Лазоренко Є.М. (ВІТІ)

АНАЛІЗ БЕЗПЕКИ СИСТЕМ МОНІТОРИНГУ ТА СПОСТЕРЕЖЕННЯ ЗА СЕРВІСАМИ ІТС ЗСУ

Актуальність. Сучасна інформаційно-телекомунікацій система (ІТС) ЗС України характеризується великою кількістю мережевого обладнання, серверів і програмних рішень, що працюють за різними стандартами та протоколами. Для отримання інформації щодо функціонування та контролю за використанням елементів ІТС розгорнуто системи моніторингу та спостереження за сервісами.

Мета. Порівняти функціональні характеристик та можливості систем моніторингу та провести аналіз безпеки сучасних СМ.

Основні положення. Система моніторингу та спостереження за сервісами – це програмне забезпечення призначене для збору, обробки, зберігання та відображення повної інформації про стан всіх компонентів телекомунікаційної і інформаційної інфраструктури мережі в реальному часі незалежно від архітектури мережі, типу обладнання і постачальників програмного забезпечення.

Для забезпечення надійної роботи телекомунікаційної інфраструктури до сучасних СМ висувають наступні вимоги: масштабування, невтручання в роботу мережного обладнання завдяки оверлейній архітектурі збору даних, підвищена безпека; підтримка розподіленої архітектури клієнт–сервер, відкритість, яка дозволяє керувати обладнанням різних виробників. На сьогоднішній день існує достатня кількість СМ, які схожі за функціоналом і надають практично однаковий набір можливостей. Проведений аналіз фунціоналу СМ з безкоштовною ліцензією представлений в табл.1.

Таблиця 1

Порівняння функціоналу систем моніторингу

Функціональність	Zabbix	Nagios	Zenoss
Даш-борди (візуалізація)	Так	Так	Так
Автоматичне виявлення загроз	Так	Через плагін	Так
Доступ через Web	Повний доступ	Огляд,звіти.	Повний доступ
Операційні системи	Windows, Linux, AIX, FreeBSD, Solaris, HP-UX, OpenBSD, SCO OpenServer, Tru64/OSF	Linux, FreeBSD, Solaris, HP-UX, AIX	Windows, Linux, FreeBSD
Моніторинг мережевих служб	SNMP v1,2,3, SSH, NTP, NNTP, LDAP, SMTP, FTP, POP3, HTTP	SNMP, NNTP, SMTP, POP3, HTTP, ICMP	SNMP, SSH, NNTP, FTP, POP3, HTTP, LDAP

СМ Zabbix має можливість взаємодіяти з пристроями різних виробників, забезпечує моніторинг мережі з великою кількістю кінцевих пристроїв та регулярно оновлюється.

До безпеки систем моніторингу сформовано наступні вимоги:

- контроль доступу та збереження цілісності даних,
- аутентифікація та перевірка привілеїв;
- підтримка ключів шифрування та управління правами;
- захист системи від атак методом перебору паролів;
- управління паролями, зовнішнім доступом та з'єднання з іншими мережами.

Висновок. **С**истема моніторингу Zabbix має більший набір функціональних можливостей порівняно з іншими системи. Виконання перелічених вимог до безпеки системи моніторингу та спостереження за сервісами ІТС забезпечить її безперервне та стійке функціонування, а також мінімізує можливість несанкціонованого доступу.

Бабарика А.О. (НАДПСУ)
д.т.н. Катеринчук І.С. (НАДПСУ)
Табенський С.М. (НАДПСУ)

ЗАСТОСУВАННЯ АЛГОРИТМІВ РОЗПІЗНАВАННЯ ОБРАЗІВ НА ОСНОВІ НЕЙРОМЕРЕЖЕВИХ ТЕХНОЛОГІЙ

Широка доступність систем відеоспостереження призвела до ситуації, коли ми маємо можливість розмістити на підконтрольних об’єктах достатньо велику кількість камер відеоспостереження, але водночас постає проблематика контролю за обстановкою з цих камер.

Оператори відеоспостереження фізично не можуть одночасно відстежувати інформацію з 10-15 та навіть більше відеоканалів.

Саме тому логічним кроком у розвитку систем відеоспостереження є впровадження функцій відеоаналітики. Одним з детекторів, які використовують в сучасних інтелектуальних системах відеоспостереження є детектор перетину умовної лінії.

Логіка роботи вказаного детектора полягає у тому, що оператор у програмному інтерфейсі будує умовну лінію, при перетині якої визначеними об’єктами (особи, транспортні засоби, чи будь-які рухомі об’єкти) відбувається візуальне (та/чи звукове) сигналізування.

Отже впровадження вказаного типу детекторів в системи відеоспостереження, які розгорнуті на об’єктах з периметральною охороною дозволить ефективно контролювати обстановку в секторах камер відеоспостереження по визначеній кількості відеоканалів одночасно.

Для супроводження об’єктів у відеопослідовностях необхідно вирішити задачу виявлення таких об’єктів.

Вирішення цієї задачі покладається на детектори об’єктів. Історично, більшість дослідницьких зусиль було зосереджено на виявленні певної категорії об’єктів, таких як пішоходи, обличчя, транспортні засоби тощо за допомогою попередньо створених наборів відповідних ознак (наприклад HOG, Haar, LBP та ін.).

Так у 2001 році P. Viola та M. Jones запропонували метод, який в режимі реального часу давав змогу виявляти обличчя на зображеннях.

Детектор Viola-Jones використовує метод розсувних вікон який дає можливість змінюючи масштаб та положення „ковзаючого вікна” виявити чи є у якомусь вікні набори пікселів що відповідають зображенню обличчя. У якості класифікатора використовують каскади Хаара.

У 2005 році N. Dalal та B. Triggs запропонували метод, який в подальшому отримав назву HOG (Histogram of Oriented Gradients).

Детектор HOG змінює масштаб вхідного зображення кілька разів зберігаючи розмір вікна виявлення незмінним. Основною ідеєю алгоритму є припущення, що зовнішній вигляд та форма об’єкта на зображенні можуть бути описані за допомогою функції розподілу градієнтів інтенсивності.

Особливістю описаних методів є те, що для класифікації фрагментів зображень виділялись вручну підібрані ознаки, тобто об’єкти виявляються за допомогою набору заздалегідь визначених шаблонів функцій.

Вказані підходи є евристичними та не виключають ймовірності вибору помилкового признака.

У 2012 році на конкурсі ImageNET впевнену перемогу отримує алгоритм оснований на використанні згорткових нейронних мереж CNN (Convolutional neural network) AlexNet і це стає переломним моментом в розвитку нейронних мереж.

Хронологію розробки найпоширеніших нейромережевих алгоритмів виявлення об'єктів в період з 2014 по 2019 роки показано на рисунку 1.

Сучасні алгоритми виявлення об’єктів на зображеннях можна поділити на категорії:
– алгоритми основані на „двоетапному виявленні”;
– алгоритми основані на „одноетапному виявленні”;
– алгоритми основані на виявленні на основі точок;
– алгоритми основані на інших авторських підходах.

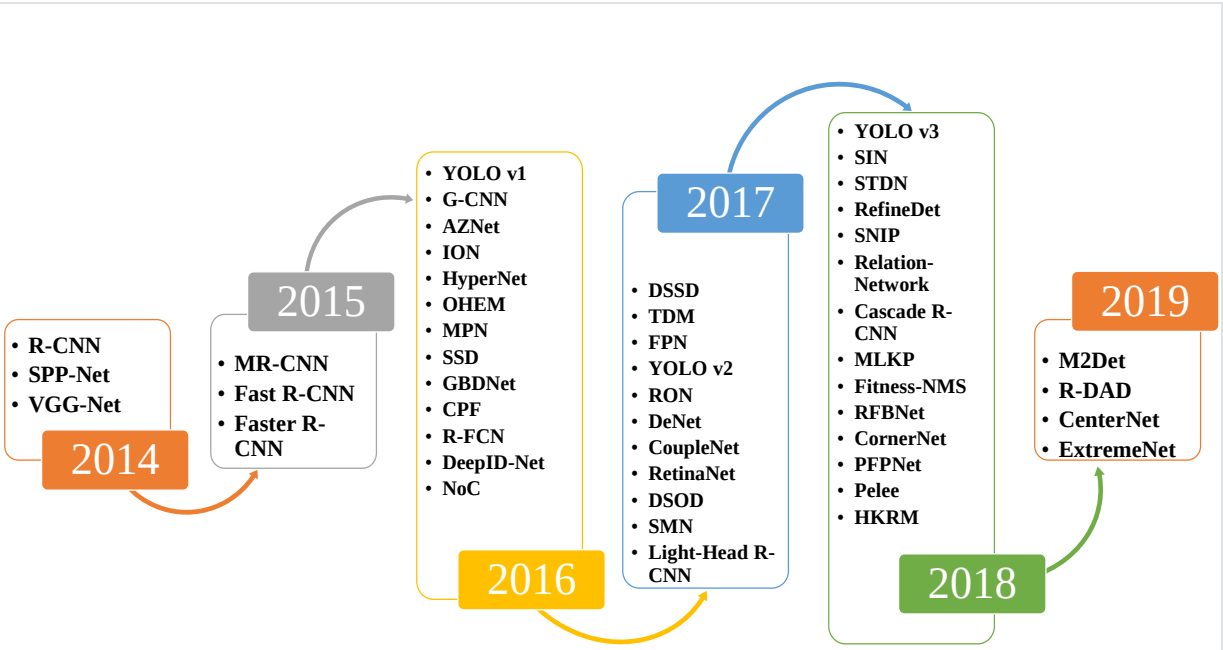


Рис. 1 – Хронологія розробки нейромережевих алгоритмів виявлення об’єктів в період з 2014 по 2019 роки

При двоетапному виявленні, алгоритмом спочатку здійснюється виділення регіонів, в яких ймовірно знаходяться об’єкти інтересу, а потім вирішується задача класифікації. Одними із перших алгоритмів, в яких було реалізовано вищеописаний механізм були R-CNN, Fast-RCNN, Faster R-CNN, Mask R-CNN та інші.

Одноетапні алгоритми вирішують задачу виявлення як задачу регресії. Такі детектори, ні відміну від двоетапних, представляють собою одну згорткову нейронну мережу, на виході якої отримуються локалізовані області об'єктів інтересу, їх класифікацію та корекцію обмежувальних рамок.

Одним з перших представників цього класу алгоритмів є YOLO. В подальшому, на основі ідей запропонованих у YOLO, було розроблено SSD, YOLOv2, YOLOv3, DSOD, RFBNet тощо.

У 2018 році дослідниками було запропоновано нові підходи до виявлення об’єктів на основі точок, та були реалізовані в алгоритмах CenterNet, CornerNet, CornerNet-Lite, ExtremeNet.

Це свідчить про стрімкий розвиток нейромережевих алгоритмів в задачах виявлення та класифікації об’єктів на зображеннях (відеопослідовностях).

Проведені експериментальні дослідження вказують на те, що для практичного застосування в програмних модулях інтелектуальних систем відеоспостереження доцільним є використання лише частини вищевказаних алгоритмів, які забезпечують швидкість обробки кадрів для відображення відеоінформації в реальному часі та не накладають суттєвих обмежень на апаратну частину серверного обладнання.

Баканов В.С. (ГІТВ ГШ ЗС України)
д.т.н. Чевардін В.Є. (ВІТІ)

ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНИХ МЕРЕЖ ЗС УКРАЇНИ

Актуальність. Досвід організації зв'язку під час проведення АТО на сході України (ООС) в черговий раз показав важливість та необхідність використання інформаційних мереж в ході планування операцій та застосування угрупувань військ ЗС України.

Виклад основного матеріалу дослідження. З початком збройної агресії на сході України інформаційні мережі спеціального призначення виконували тільки базові функції: телефонний зв'язок, відео конференційний зв'язок та передачу даних і не задовольняли потреби ЗС України. Починаючи з 2014 року уряд США розпочав програму допомоги ЗС України щодо розвитку існуючих та створення нових інформаційних систем, сумісних зі стандартами НАТО. Одним з найважливіших та значущих проектів є Програма Уряду США з впровадження рішень на основі інформаційних технологій для ЗС України (USAI-IT), яка включає 3 етапи реалізації.

Перший етап включає: розгортання інформаційних мереж (U-NIPR та U-SIPR), розгортання серверної, мережевої інфраструктур, базових ІТ - сервісів на Головному ІТВ (ЦОД) ЗС України, розгортання та налаштування функціональних систем: центру оперативного управління і контролю (С2С), центру оперативного реагування на кібернетичні загрози (CSOC), медичної інформаційної системи (MIS), логістичної інформаційної системи (LIS). Другий етап включає: розгортання серверної, мережевої інфраструктур, базових ІТ – сервісів на резервному ЦОД ЗС України, розгортання резервного центру оперативного управління і контролю (С2С) та розгортання ІТ – інфраструктура на окремих об'єктах ЗС України. До третього етапу входять навчання та технічна підтримка.

Система військового управління і контролю (С2С) – це модульне, клієнт-серверне програмне забезпечення (Life Ring), що дозволяє здійснювати обмін інформацією між базами даних з метою створення шарів оперативної обстановки та загальної оперативної картини на електронній карті, є сумісною з системою „Дельта" та підтримує моделі обміну даних НАТО (ADEM та NATO Vector Graphics).

Логістична інформаційна система (LIS) – це система записів та звітів, що використовуються для агрегування, аналізу, перевірки та відображення даних підтримки рішень логістичного забезпечення. Підтримує всі основні аспекти управління процесами для 5 класів постачання згідно класифікації НАТО, сумісна з логістичною системою НАТО (LOGFAS).

Медична інформаційна система (MIS) – це програмне рішення, що застосовується для підтримки ЗС України на щоденній основі та в районах проведення ООС. MIS надає можливість обмінюватися електронними даними, зберігати інформацію про пацієнтів, їх документи, особливості переміщень між медичними закладами, дані про госпіталізації та дослідження, підтримує стандарти Allied Joint Medical Support Doctrine.

Центр оперативного реагування на кібернетичні загрози (CSOC) забезпечує захист мереж за допомогою брандмауерів, централізоване управління брандмауерами (Firepower), тестування мереж на вразливості (Metasploit), моніторинг несанкціонованої поведінки користувачів (Forcepoint Insider Threat), захист від втрати інформації (Forcepoint Data Loss Prevention), захист від вірусів (ESET), створення журналів подій (Arcsight).

Висновок. Таким чином, реалізація програми USAI-IT дозволила за рахунок розширення спроможностей підвищити ефективність інформаційних мереж ЗС України та досягти визначених показників безпеки інформації відповідно стандартів НАТО. Було започатковано кардинально новий підхід щодо управління військами, логістики та медичного забезпечення, що значною мірою спрощує взаємодію між всіма ланками управління.

к.т.н. Барановський О.М.(НТУУ „КПІ”)
к.т.н. Жилін А.В. (НТУУ „КПІ”)
Новіцький І.Ю. (НТУУ „КПІ”)

МЕТОДИКА ВИЯВЛЕННЯ ЗЛОЯКІСНОГО ТРАФІКУ НА ОСНОВІ ПОВЕДІНКОВОГО АНАЛІЗУ

Актуальність. Поширення засобів автоматизації при передачі й обробці інформації, а також в управлінні й прийнятті рішень призводить до зміщення акценту кібератак. Це зміщення відбувається від добре захищених серверів та робочих станцій до вразливих на рівні операційних систем та систем введення-виведення інформації мережевих та периферійних пристроїв. Ці пристрої після зараження слугують майданчиком для подальших атак та віддаленого доступу. При цьому непопулярність антивірусного програмного забезпечення для мережевих та периферійних пристроїв призводить до **постановки задачі** щодо необхідності розробки нового підходу у виявлені в мережевому трафіку ознак впливу шкідливого програмного забезпечення не стільки на основі сигнатурного аналізу, скільки з врахуванням поведінки об’єктів мережі.

Мета. Розробка методики виявлення злоякісного трафіку на основі поведінкового аналізу, який ґрунтується на прийнятті рішення щодо виду мережевого трафіку на основі кореляції зібраного NetFlow та оцінок від різних алгоритмів машинного навчання, що використовують правила snort для свого навчання.

Основні положення. Зазвичай системи виявлення аномалій у мережевій поведінці використовуються разом зі звичайними мережевими екранами та застосунками для виявлення шкідливих програм. Деякі виробники визнають, що системи виявлення аномалій у мережевій поведінці є частиною їх рішень з мережевої безпеки. Зазначені системи також використовують аналіз журналів реєстрації подій, аналіз пакетів, моніторинг мережевих потоків та аналіз маршрутів. Під час виявлення аномалій у мережевій поведінці проводиться безперервний моніторинг мережі на наявність незвичних подій або тенденцій

Під час дослідження було проаналізовані основні методи виявлення злоякісного трафіку з хостів в мережі. Встановлено, що моніторинг роботи мережі зображує мережевий трафік як сукупність потоків пакетів, що обмінюються в TCP/UDP-з’єднаннях між підключеними системами. Запис потоків може відбуватися також на межі мережі, на маршрутизаторах або на виділених системах моніторингу. При цьому він може здійснюватися локально в будь-якій системі, як моніторинг діяльності мережі, і записувати всі мережеві з’єднання, що походять з моніторингової системи або призначені для неї. Було проаналізовано роботу алгоритмів машинного навчання, а саме наївний баєсів класифікатор, випадковий ліс, C5.0. За допомогою програмного забезпечення nfdump було зібрано потоки трафіку з різним шкідливим програмним забезпеченням. Зважаючи на швидкість та масовість кібератак постала необхідність координувати свої дії з багатьма компаніями та організаціями, тому було проаналізовано стандартизовані описи атрибутів компрометації такі як: PCAP, CEF, NetFlow, YARA, CVE; та формати звітів такі як: CSV, XML, JSON. В наслідок чого створено оптимальну модель для класифікації трафіку.

Висновок. Отже, на основі аналізу різних методів детектування шкідливого програмного забезпечення було розроблено методику виявлення злоякісного трафіку на основі поведінкового аналізу, який ґрунтується на прийнятті рішення щодо виду мережевого трафіку на основі кореляції зібраного NetFlow та оцінок від різних алгоритмів машинного навчання, що використовують правила snort для свого навчання. Розроблена методика дає можливість виявляти злоякісний трафік який передається в зашифрованому вигляді та реагувати на атаки нульового дня.

к.т.н. Барановський О.М. (НТУУ „КПІ”)
к.т.н. Жилін А.В. (НТУУ „КПІ”)
Пилипенко О.В. (НТУУ „КПІ”)

МЕТОД ВИЯВЛЕННЯ ФЕЙКОВИХ БАЗОВИХ СТАНЦІЙ НА ОСНОВІ АНАЛІЗУ ПАРАМЕТРІВ ПЕРЕВИБОРУ СТАНЦІЙ ТА РАДІОЕЛЕКТРОННОЇ ОБСТАНОВКИ

Актуальність. Атака через зловмисну базову станцію (FBS) – це добре відома атака, яка може компрометувати конфіденційність користувачів, відстежуючи їх географічне місцеположення, перехоплювати персональну інформації користувачів тощо. Дешеву базову станцію можливо створити за допомогою USRP. Зростання популярності USRP призвело, наприклад до дешевої реалізації атак фальшивих базових станцій. Тому **постає задача** розроблення методу ідентифікації фейкових базових станцій на основі аналізу параметрів зі службових каналів.

Мета роботи: дослідження методів виявлення фейкових базових станцій, які існують на теперішній час, їх недоліків та розробка більш досконалого методи ідентифікації FBS на основі попередніх методів.

Основні положення. Було проаналізовано існуючі методи щодо виявлення фейкових станцій. Їх недоліки полягають або в слабкій аутентифікації базової станції кінцевими пристроями, або в значних ресурсних затратах на розгортання інфраструктури. Запропонований способів виявлення ґрунтується на збирані інформації з багатьох базових станцій, щоб сформувати „fingerprint” того, що є нормальною роботою. Відхилення від цих показників можна вважати підозрілим. Виявлення підозрюваної поведінки починається зі збору трафіка. Потрібно мати можливість приймати та обробляти сигнали GSM, UMTS, LTE. Це можна зробити за допомогою пристрою USRP N210 та ноутбуку з операційною системою Ubuntu 16.4+. В ході аналізу та поставленого експерименту були встановлені наступні основні параметри для виявлення фейкових базових станцій:

1. LAC, який використовуються в даній місцевості. Якщо один виділяється іншими LAC, це підозріло.
2. Крім того, дуже низькі значення T3212 є підозрілими. Це значення призведе до дуже частого оновлення місцеположення, що не дасть користувачу підключитись на іншу станцію.
3. Особливо сильні сигнали, які з’являються на невеликій території, можуть вказувати на невеликий локальний IMSI-catcher.
4. Наявність дуже високих значень CRO.
5. Наявність низьких значень TO.
6. Наявність низьких значень PT.
7. Низькі значення MX_TXPWR_MAX_CCH.
8. Наявність низьких значень RXLEV_ACCESS_MIN.
9. Високі значення CRH.
10. Пустий neighbors list.

Висновок: В роботі було проаналізовано роботу IMSI catchers та FBS, а також стандартів зв’язку GSM, UMTS, LTE. Працюючу FBD було створено, і вона була протестована у реальних умовах. Результатом експерименту є те, що мережевий трафік трансляції в реальній та фейковій базовій станції дуже схожий. Фактично в трафіку, що походить від стільника з тим самим MNC, всі параметри, які не пов’язані з ідентифікацією, були однакові. Це вказує на те, що намагатися „fingerprint” трансляційного трафіка не дуже ефективний метод. Проте параметри перевибору BTS – різні, та їх можливо побачити і проаналізувати. Але, на жаль, експеримент був проведений лише у невеликій географічній області. Збір інформації слід робити з більших місцеположень, щоб з’ясувати параметри конфігурації мережі в сусідніх стільниках, а також залучити до цього більше пристроїв USRP.

к.г.н. Бардін О.О. (в/ч А4444)
Немченко О.О. (ТОВ „Вейт”)

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ БОЄПРИПАСІВ ТИПУ „УДАРНЕ ЯДРО” ДЛЯ САМОЗАХИСТУ СУХОПУТНИХ БОЙОВИХ ПЛАТФОРМ

Нині, одним з найважливішим, невід’ємним компонентом бойових систем є повітряні дрони, до яких відносяться різноманітні безпілотні літальні апарати (розвідувальні, ударні, ретрансляційні, тощо). На черзі широке впровадження роботизованих, наземних, сухопутних бойових платформи (сухопутних дронів). Перспектива безальтернативної роботизації озброєння, покроковий перехід від дистанційно керуємо апаратів до оснащених штучним інтелектом, самостійно діючих бойових машин має наступні важливі підстави.

Актуальність проблеми. Життя бійця є найвища цінність держави. У зв’язку з цим заміна бійців на особливо небезпечних напрямках (розвідка, розмінування, транспортування боєприпасів, тощо) роботизованими платформами здійснюється усіма арміями розвинутих держав. На сей час, бойові, дистанційно керуємо апарати різного рівня автономності активно створюються не тільки для повітряного, але і наземного, надводного і підводного простору.

Вміння наносити удари і захищати себе при виконанні бойового завдання, в тому числі при безпосередньому зіткненні з противником, є найважливішою властивістю бойового сухопутного дрона. Пошуку ефективної конфігурації захисного озброєння сухопутних дронів, які можуть бути висунути на нейтральну полосу (сіру зону) з розвідувальним завданням, при цьому ефективно захищати себе, присвячена ця публікація.

Останні досягнення „Укроборонпрому”. Розглянемо наукові засади вирішення визначеної проблеми на прикладі створеного в „Укроборонпроме” безпілотного, дистанційно керуємо транспортного засобу на броньованій колісній платформі – бойовий, сухопутний дрон „Фантом”. Цей багатофункціональний дрон вже оснащений засобами боротьби з живою силою і бронетехнікою противника і може діяти в авангарді наших сил, здійснюючи розвідку при наступі. Проте, знаходячись в глибокому, одиночному розвідувальному рейді, діючи у відриві від основних сил, дрон „Фантом” має підвищені ризики нападу. Аналізуючи досягнутий рівень самозахисту, можливості самостійної боротьби дрона „Фантом” з танками, БМП, БТР та бронеавтомобілями супротивника, а також можливості пересування по бездоріжжю, можна відзначити наступне.

Базовий варіант дрона „Фантом”, має колісну формулу 6×6 і може пересуватися по бездоріжжю і піску. Його більш досконала модифікація „Фантом-2” має колісну формулу 8×8, і може бути оснащений гусеницями, тобто мати можливість пересування у надскладних умовах бездоріжжя. Гібридний двигун, повний привід і незалежна підвіска колісної бази, а також гідравлічна гальмівна система забезпечує „Фантому” високі ходові характеристики. Запас ходу міні-БТР „Фантом-2” досягає 130 км, потужність гібридного двигуна близько 80 кВт, швидкість до 60 км/ч. Управління здійснюється по захищеному радіоканалу, дальність якого досягає 20 км без використання розміщених на БпЛА ретрансляторів, та одночасно через оптоволоконний кабель довжиною до 2 км, який дає практично необмежені можливості по передачі інформації.

„Фантом-2” укомплектований стабілізованою поворотною платформою на якої може розміщено різноманітне озброєння. Це кулемет калібром 12,7 мм, спарена 23-мм гармата, система залпового вогню некерованими ракетами РС-80, а також дві пускові установки для керованих протитанкових ракет Р-2 комплексу „Бар’єр”, здатних вражати цілі на відстані від 100 до 5000 метрів. За припущенням розробників, основне застосування сухопутного дрона „Фантом-2” це розвідка та знищення танків з засади, хоча можливі й інші варіанти його застосування.

Важливи переваги над прототипами. Як вже вказано, певною перевагою „Фантом-2” над відомими прототипами є наявність високошвидкісного і високопродуктивного оптоволоконного каналу зв’язку, який дозволяє встановити різноманітну оптичну апаратуру,

в тому числі HD-якості. Практика довела, що в існуючих умовах, незважаючи на вразливість оптоволоконного кабелю, штучних пошкоджень у ході випробувань не спостерігалося.

Сумеречна оптика, тепловізори, реєстратори модульованого лазерного випромінювання, мікрохвильові локатори, високо чутливі мікрофони направленої дії, сейсмоакустичні датчики – це далеко не повний перелік додаткового обладнання, що дозволяє створити на базі „Фантом-2" ефективний розвідувальний засіб переднього краю, через який можна координувати дію інших сухопутних бойових платформ.

Бойова платформа „Фантом-2", будучи висунутої на 1,0÷1,5 км вперед від рубежа оборони, в перспективі, може, за допомогою відповідного пристрою, здійснювати постановку хибних оптичних растрових завад, включення яких здійснюється автоматично, за командою датчика який здатний реєструвати ультрафіолетове випромінювання ракетного посліду. Внаслідок попадання в зону більш інтенсивного поля лазерної розвертки з хибними командам ПТУРи класу „КОРНЕТ" (РФ) з лазерним наведенням, які летять в сторону наших позицій, будуть втрачати керування.

Також важливою перевагою схеми керування „Фантом-2" є наявність другого оператора, який веде стрільбу з кулемета, керує ракетним та іншим озброєнням. Таким чином, будучи висунутим на передній край, на деякий танко-небезпечний напрямок, „Фантом-2"може не тільки вести бій з танками, але і з супроводжуючи їх піхотою, тобто реалізувати принцип „найкраща броня це влучний постріл на упередження". Таким чином, за наявністю дистанційного водія і оператора-стрілка „Фантом-2"набуває функції безпілотного міні-БТР. Існуюча конфігурація корпусу дозволяє, наприклад, здійснити монтаж навісних, імпульсних, широко кутових бортових мінівогнеметів, бортових мортир малого калібру, що дозволять захистити „Фантом-2"від прямого контакту з ДРГ противника. В особливо критичній ситуації не виключено включення модуля самоліквідації (разом з нападниками).

Існуючі недоліки і шляхи їх усунення. Однак є проблема. Змонтований на платформі „Фантом-2" протитанковий комплекс „Бар'єр" бореться з танками і БМП на дистанції 100÷5000 метрів. Таким чином, дистанція 0÷100 метрів є зоною ураження від бронетехніки противника. Виникає питання – як захистити дрон „Фантом-2"на дистанції прямої видимості? Одним з можливих варіантів, це застосування боєприпасів типу „ударне ядро", яке необхідно розміщувати на деякому віддаленні від „Фантом-2" для захисту оптики і навісного озброєння від спалаху заряду, або безпосереднє на корпусі, при реалізації захисних заходів.

Оцінка параметрів „ударного ядра". Як зразок для створення протибортової міни для комплектації „Фантом-2", що діє на принципі ударного ядра, можна розглянути міну ТМ-83, яка має вагу 28,1 кг, масу заряду (ТГ-40/60) 9,6 кг, габарити 45,5х37,7х44,0 см. Дальність ураження цілі від 5 до 50 метрів, пробиваємось броні близько 100 мм, діаметр пробоїни близько 80 мм. Міна має комбінований сейсмічно-оптичний детонатор, з сейсмічним датчиком ВТ-02 і оптичним датчиком ВТ-01. Однак, міна може встановлюватися тільки вручну, що і перешкоджає її застосуванню сухопутним роботом без додаткового удосконалення. У зв'язку з цим постає питання про обгрунтування параметрів для розробки вдосконаленого боєприпасу типу „ударне ядро", серйозним достоїнством якого є простота виготовлення і дешевизна.

Згідно оціночних показників, в ідеальних умовах „ударне ядро" має наступні теоретичні характеристики. Якщо прийняти діаметр боєприпасу D=240 мм, то діаметр ядра вражаючого елемента складе близько d=D/4≈60 мм, з масою порядку M≈1,5 кг і швидкістю V≈2,5 км/с. Формування ядра завершується на дистанції близько s=10×D=2,4 м. Теоретично „ударне ядро" зберігає деяке бронепробиття до дистанції порядку S=1000×D≈240 м. Теоретична бронепробійність на оптимальної дистанції складає біля S=D*2≈480 мм.

Природно, що це тільки теоретичні параметри, які у реальності залежать від точності виготовлення, рівня однорідності вибухової речовини, ефективності кумуляції, повітряного середовища, кута атаки і т.п. Однак, можна припустити, що незважаючи на аеродинамічну недосконалість „каплі псевдорідинного металевого ударного ядра" і втрачу швидкості від

тертя об повітря, на дистанції до 100 м боєприпас типу „ударне ядро” діаметром 240 мм забезпечить захист дрона від ворожої бронетехніки навіть у фронтальній проекції. До речи, кумулятивний заряд КЗД-100 (РФ) зберігає бронепробійність до дистанції 100 м, хоча більшість протибортових мін (МРВ, Польща; Mi-AC-AH, Франція; ІНМ, ЮАР; Krakatoa, Великобританія та ін.) гарантують бронепробійність до дистанції 50÷80 м.

Варіанти застосування захисного озброєння. Основна проблема при використанні боєприпасів типу „ударне ядро” це наявність спалаху вибухової речовини, здатної пошкодити оптику і інші елементи конструкції при розміщенні міни безпосередньо на платформі „Фантом-2”. Це вимагає прийняття відповідних конструктивних рішень, або розміщення протибортової міни за допомогою штатива, безпосередньо на ґрунті.

Припустимо, що міні-БТР „Фантом-2”несе на зовнішній підвісці дві керуючі міни типу „ударне ядро” вагою близько по 20 кг, кожна з яких оснащена високочутливим датчиком центра магнітної маси, телевізійним прицілом, механізмом наведення, котушкою з кабелем, який з’єднує виносний боєприпас з базовою платформою „Фантом-2” і через який забезпечується ретрансляція сигналів. Розмістивши міни на ґрунті „Фантом-2”вибирає позицію, коли він знаходиться під захистом виносних боєприпасів, він може вибрати кабель і перейти в режим спостереження, очікуючи бронетехніку противника.

Наступним варіантом є розміщення на броні некерованих протитанкових снарядів класу РПГ-7 (постріл ПГ-7В), РПГ-29 „Вампір” (постріл ПГ-29В), прицілювання якими здійснюється оператором. Можливі й інші варіанти

Порівняльна оцінка бойових платформ.Необхідно відзначити, що реальна практика застосування російських сухопутних дронів “Уран-9” в Сирії, в умовах реальних бойових дій, не була такою успішною, як передбачалося. Новий білоруський бойової дрон „Берсерк” обкатку боєм не пройшов. Це дає шанс, по відношенню до наших найближчих конкурентів, провести обкатку міні-БТР „Фантом-2” в реальній бойовій обстановці на південному сході України і вийти на ринок озброєння з високо конкурентною продукцією. У зв’язку з цим на перший план виходять питання ретельного і всебічного випробування сухопутних дронів, спільна робота з конструкторами по усуненню недоліків, грамотна підконтрольна експлуатація в ході фронтових операцій на сході України.

Зрозуміло, що розробка роботизованих сухопутних дронів (колісних, гусеничних, крокуючих), буде неминуче тривати, в тому числі у варіанті, коли в одному строю будуть керовані людьми бронемашини і роботизовані бойові платформи. Швидше за все, як і в безпілотної авіації, буде створений весь номенклатурний ряд бойових дронів – мікро, міні, мідл, макро і т. д., з усезростаючим рівнем штучного інтелекту. Тому дуже важливо не втратити пріоритет існуючих досягнень.

Висновки і пропозиції. Проведений аналіз довів перспективність застосування боєприпасів типу „ударне ядро” для боротьбі з бронетехнікою противника на дистанції прямої видимості, унаслідок чого доведена доцільність здійснення дослідно-конструкторських робот у цьому напряму.

Практика довела, що зграя повітряних дронів діє дуже ефективно. Можливо це стосується і сухопутних дронів, що потребує не тільки додаткового вивчення, а й практичної апробації. Наступний фактор це доведена необхідність безперервного вдосконалення обчислювального обладнання міні-БТР „Фантом-2”, аж до рівня штучного інтелекту, який самостійно визначає шлях пересування, виконує класифікацію „свій-чужий”, обирає зброю, дистанцію, виконує прицілювання, ураження, аналіз результатів, визначає наступні дії згідно основного завдання, а також координує дію інших бойових платформ через захищений від електромагнітних завад оптоволоконний кабель.

Необхідне підкреслити, що міні-БТР „Фантом-2”, це безумовний прорив України на міжнародному ринку озброєння. Тому друге завдання публікації – звернути увагу керівництва на цю розробку, яка поки що випереджає за своїм рівнем найближчих конкурентів, і, яка потребує державної підтримки для подальшого вдосконалення даного перспективного зразка робототехніки.

Басанець Д.О. (ВІТІ)
Кирган О.О. (ВІТІ)

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ АНАЛІЗУ СТАТИСТИЧНИХ ДАНИХ З ОБЛІКУ МАТЕРІАЛЬНИХ ЗАСОБІВ У КВАРТИРНО-ЕКСПЛУАТАЦІЙНІЙ СЛУЖБІ

Аналіз даних є науковим методом дослідження об'єкта через розгляд його боків, властивостей і складових частин. Використання достовірної і науково-обгрунтованої інформації приводить до зменшення витрат, підвищення якості та ефективності роботи квартирно-експлуатаційної служби по обліку матеріальних засобів.

Обробка великих масивів необхідна для аналізу діяльності, та може бути виконана лише з використанням сучасних засобів інформаційних технологій в програмному забезпеченні. Організація квартирно-експлуатаційного забезпечення ЗС як комплекс заходів, спрямований на безпечну експлуатацію, утримання казармено-житлового фонду, об'єктів соціально-культурного призначення, забезпечення військових частин квартирним майном.

На квартирно-експлуатаційну службу покладається:

1. забезпечення економного споживання палива, води, електроенергії та газу, а також матеріалів, які виділяються на квартирно-експлуатаційне забезпечення та ремонтно-будівельні роботи;
2. організація збереження та матеріальний облік фондів і територій військових містечок, квартирного майна та земельних ділянок, переданих військовій частині на утримання та експлуатацію, проведення їх інвентаризації;

Особлива увага сконцентрована на вирішення забезпечення військовослужбовців і службовців сучасним ремонтом будівель і приміщення та удосконалення навчально-матеріальної бази, реконструкцію старих об'єктів.

Щоб надати певним службам їх повноважень та виконання деяких дій у системі обробки даних та засоби доступу до певного захищеного ресурсу було створено авторизацію. До авторизації входить так як автентифікація так і ідентифікація. Для кожного авторизованого користувача була створена таблиця з даними.

Щоб зберегти всі дані які були отримані від служб для аналізу використовуємо веб-додаток *phpMyAdmin* з яким ми зможемо адмініструвати бази даних *MySQL*, переглядати вміст таблиць баз даних. Цей додаток зручним тим, що дозволяє керувати базу даних *MySQL* без вводу *SQL* команд через інтерфейс.

Використовуючи дані з таблиць за допомогою програмного забезпечення ми можемо порівняти дані які хоче дізнатися користувач.

Для оцінювання показника , необхідно розраховувати її річного утримання. Для цього використали теорію калькулювання витрат. В нашому випадку під калькулюванням слід розуміти обчислення собівартості окремих заходів КЕС за рік. В якості об'єкту калькулювання виступають заходи діяльності служби, вартість яких обчислюється в конкретному році.

Перевагами програмного забезпечення аналізу статистичних даних КЕС є:

1. Швидкий аналіз витрат та утримань особового складу;
2. Прискорення проведення інвентаризації майна;
3. Зручна авторизація користувача, та надання йому повноважень.

Таким чином, програмне забезпечення аналізу даних КЕС дозволив виділити такі статті витрат: витрати на утримання особового складу, витрати на утримання будівних споруд, витрати на утримання та обслуговування техніки й обладнання КЕС, вартість витрат ресурсів КЕС. Завдяки використанню комп'ютерів і сучасного програмного забезпечення, оброблення й аналіз даних став набагато легшим. При цьому для застосування основних статистичних методів оброблення даних людям не потрібно заглиблюватися в складність математичних процедур, а варто зрозуміти, для чого і як ці методи використовуються, а також вміло використовувати обраний пакет прикладних програм.

Безносенко С.Ю . (НЦЗІ ВІТІ)
Добропас Б.І. (НЦЗІ ВІТІ)
Білий О.А. (НЦЗІ ВІТІ)
Пономаренко З.М. (НЦЗІ ВІТІ)

ШЛЯХИ УДОСКОНАЛЕННЯ СИСТЕМИ МЕТРОЛОГІЧНОГО ОБСЛУГОВУВАННЯ ВІЙСЬК ЗВ'ЯЗКУ

Актуальність. Досвід виконання завдань військами зв'язку в операції об'єднаних сил на території Луганської та Донецької областей ще раз підтвердив важливість своєчасного виконання в польових умовах таких заходів, як – вимірювання параметрів і характеристик при технічному обслуговуванні, проведення встановлених для них видів ремонту комплексних об'єктів зв'язку і АУВ, що дозволяє своєчасно повернути до строю той чи інший зразок техніки.

Виклад основного матеріалу дослідження. Метрологічне обслуговування – це комплекс заходів, спрямованих на досягнення єдності вимірювань та достовірності контролю параметрів об'єктів вимірювань військового призначення.

Загальні положення, основні визначення, термінологія і поняття метрологічного забезпечення регламентуються законодавчими актами України та нормативно-правовими актами Міністерства оборони України, основними з яких є:

Функціонування системи метрологічного забезпечення Збройних сил України забезпечується законодавчими актами України та нормативно-правовими актами Міністерства оборони України, основні з яких перелічені вище. Вказана нормативно-правова база дала змогу створити структуру метрологічної служби Міністерства оборони та Збройних сил України, яка спроможна виконати комплекс заходів з метрологічного обслуговування озброєння та військової техніки та забезпечення військ вимірювальною технікою, без врахування метрологічного обслуговування сучасних засобів зв'язку.

На сьогоднішній день система метрологічного забезпечення ЗС України має наступну структуру:

органи військового управління:

на стратегічному рівні – Центральне управління метрології і стандартизації Збройних Сил України Озброєння Збройних сил України;

на оперативно-стратегічному рівні – служби метрології і стандартизації видів ЗС України (Сухопутні війська, Повітряні сили, Військово-морські сили);

на оперативному рівні – служби метрології і стандартизації оперативних командувань, Повітряних Командувань, Військово-морські бази ВМС;

на тактичному рівні – служби метрології та стандартизації військових частин.

На жаль на оперативному рівні у військах зв'язку не створена служба метрології і стандартизації (приклад в ССО СМіС складається з 1 військовослужбовця).

Технічні засоби зв'язку старого парку, які є у військових частинах (підрозділах) та установах практично не використовуються ні в стаціонарних умовах, ні в польових, ні в умовах проведення ООС.

Натомість у військових частинах та районі проведення ООС широко використовуються сучасні засоби зв'язку.

З метою узагальнення параметрів, які повинні підлягати вимірюванням, наявності документації з метрологічного обслуговування та засобів вимірювань необхідних для цього, сучасні засоби зв'язку можна розділити на групи: засоби зв'язку виробництва компанії Motorola та виготовлених на їх базі виробів Либідь засоби зв'язку виробництва компанії Harris; комплекти станцій супутникового зв'язку компанії "Tooway"; волоконно-оптичні системи передачі; телекомунікаційні комплекти ТК-1, ТК-2, ТК-3, ТК-4; апаратура цифрового радіорелейного зв'язку; радіорелейна станція Р-425С3; радіорелейна станція Р-402 (СРШ-5000).

На цей час у військах зв’язку метрологічне забезпечення в наступному стані:

1. Наявність та відповідність документації з технічного обслуговування.

На різні групи сучасних засобів зв’язку існують різні проблеми:

документація з технічного обслуговування відсутня взагалі;

документація з технічного обслуговування в наявності, але не визначені параметри, що підлягають вимірюванням;

документація з технічного обслуговування в наявності, параметри, що підлягають вимірюванням, визначені, але не в повному обсязі, або невірно;

документація з технічного обслуговування в наявності, параметри, що підлягають вимірюванням, визначені вірно та в повному обсязі, але відсутній детальний алгоритм проведення вимірювань з визначенням переліку необхідних засобів вимірювання.

2. Наявність засобів вимірювальної техніки.

У зв’язку з тим, що в документації з технічного обслуговування відсутній перелік засобів вимірювальної техніки для проведення вимірювання параметрів сучасних засобів зв’язку існує необхідність визначення конкретних типів засобів вимірювань з відповідними параметрами. Основний парк вимірювального обладнання, що знаходиться в експлуатації, створений і випускався десятки років тому, а модернізація та оновлення вимірювального обладнання відбуваються повільно і в основному за рахунок закупівель в інших країнах.

3. Наявність та підготовка особового складу.

Для проведення метрологічного обслуговування існує необхідність в наявності та підготовці особового складу. Не визначено підрозділи, які будуть проводити метрологічне обслуговування, організації, які будуть проводити їх навчання та порядок його проведення. Не відпрацьований порядок підготовки особового складу як на засобах вимірювальної техніки (в організаціях, які будуть її поставлять, або у визначених спеціалізованих організаціях), так і на сучасних засобах зв’язку за допомогою засобів вимірювальної техніки (в підприємствах-виробниках, їх представників або у визначених спеціалізованих організаціях).

4. Наявність замовлень на науково-дослідні та дослідно-конструкторські роботи у галузі метрологічного забезпечення.

Для проведення науково-дослідних та дослідно-конструкторських робіт у галузі метрологічного забезпечення для військ зв’язку невизначено пріоритетні напрямки в цій галузі та організації, які мають право виступати замовниками, робити замовлення вказаних робіт.

Отже, аналіз стану системи метрологічного забезпечення у військах зв’язку показав наступне:

військові частини та установи військ зв’язку засобами вимірювальної техніки необхідних для проведення вимірювань та контролю параметрів сучасних засобів зв’язку не укомплектовані;

технічне обслуговування зразків сучасних засобів зв’язку проводиться не в повному обсязі (не проводяться вимірювання параметрів зразків);

метрологічне обслуговування зразків сучасних засобів зв’язку не проводиться взагалі;

підрозділи (військові метрологічні лабораторії) або підготовлені фахівці, які повинні проводити метрологічне обслуговування відсутні;

документація з технічного обслуговування сучасних засобів зв’язку з детальним алгоритмом проведення вимірювання параметрів відсутня;

у зв’язку з відсутністю замовлень науково-дослідні та дослідно-конструкторські роботи у галузі метрологічного забезпечення не проводяться;

метрологічна експертиза документації на всіх етапах життєвого циклу зразків сучасних засобів зв’язку не проводиться.

Висновок. З метою якісного проведення діагностування та метрологічного обслуговування новітніх (цифрових) засобів зв’язку особовим складом Науково-дослідної

лабораторії (метрологічного забезпечення) НДВ-24 НЦЗІ ВІТІ розроблений алгоритм створення ефективної системи метрологічного обслуговування військ зв'язку, що включає:

1. Проведення детального аналізу сучасного стану метрологічного обслуговування військ зв'язку, в якому визначити:

стан забезпечення військових частин та установ військ зв'язку засобами вимірювальної техніки необхідних для проведення вимірювань та контролю параметрів новітніх засобів зв'язку;

наявність підрозділів, які проводять метрологічне обслуговування;

стан проведення метрологічного обслуговування;

наявність у військових частинах та установах підготовлених фахівців для проведення вимірювань та контролю параметрів новітніх засобів зв'язку;

наявність документації з технічного обслуговування новітніх засобів зв'язку.

2. Визначення переліку наявних у військових частинах засобів зв'язку старого парку та новітніх засобів зв'язку, наявності документації та засобів вимірювальної техніки для проведення метрологічного обслуговування.

3. Розробку детальних інструкцій з проведення метрологічного забезпечення як розділу інструкцій з технічного обслуговування.

4. Визначення переліку засобів вимірювальної техніки необхідних для проведення метрологічного обслуговування з визначенням технічних характеристик, конкретних типів, вартості та можливості їх повірки в метрологічній службі ЗСУ та в органах Держспоживстандарту.

5. Закупівлю (або тимчасову оренду) засобів вимірювальної техніки необхідних для проведення метрологічного обслуговування в одиничних екземплярах (для проведення досліджень та практичного проведення вимірювань).

6. Проведення метрологічного обслуговування наявних новітніх засобів зв'язку для виявлення організаційних або технічних недоліків та надання пропозицій на місцях дислокації військ за допомогою закуплених (або орендованих) засобів вимірювальної техніки

7. Визначення фактичного часу на проведення метрологічного обслуговування у людино/годинах.

8. Проведення навчання особового складу, який задіяний у проведенні робіт з метрологічного обслуговування.

9. Розробку мобільного комплексу для проведення метрологічного обслуговування у місцях дислокації військ.

З метою реалізації даного алгоритму та вирішення питань щодо удосконалення системи метрологічного забезпечення військ зв'язку була проведена робота в обсязі НДР „Система метрологічного забезпечення військ зв'язку" та, на даний час, ведеться робота по створенню переносного комплексу вимірювальних засобів для проведення метрологічного обслуговування засобів зв'язку.

В подальшому планується розробка комплексу, який має за мету практичне вирішення вище зазначених питань, що дозволить якісно проводити діагностування та метрологічне обслуговування новітніх (цифрових) засобів зв'язку.

ЛІТЕРАТУРА:

1. Фунтиков А.Г. Научные основы эксплуатации войсковых средств измерений : [учебн. пособие] / А.Г. Фунтиков. – М.: Военное издательство, 1988. – 240 с.

2. Исследование и обоснование развития средств измерений и контроля военного назначения: отчет о НИР (промежуточный). ВНМЦ (ВЭ). – № 202/197. – Харьков, 1996. – С. 7 – 10.

3. Коротков Б.В. Шляхи підвищення ефективності управління метрологічним забезпеченням військ (сил) / Б.В. Коротков, О.О. Морозов, С.Т. Черепков // Український метрологічний журнал. – 1998. – № 2. – С. 52 – 55.

д.т.н. Бессалов А.В. (НТУУ „КПІ”)
д.т.н. Ковальчук Л.В. (НТУУ „КПІ”)
к.т.н. Кучинська Н.В. (НТУУ „КПІ”)
Теліженко О.Б. (ООО Verum Visum)

ОБҐРУНТУВАННЯ КРИПТОГРАФІЧНОЇ СТІЙКОСТІ АЛГОРИТМУ ІНКАПСУЛЯЦІЇ КЛЮЧА, ЩО ПРОПОНУЄТЬСЯ ДО СТАНДАРТИЗАЦІЇ

Актуальність. Асиметричні методи криптографії дозволяють досить „елегантно” розв’язувати задачу розподілу ключів. Проте відповідні криптографічні перетворення працюють в алгебраїчних системах з великими значеннями параметрів, що пов’язано з виконанням затратних операцій. Порівняний аналіз швидкодії арифметики для різних типів еліптичних кривих, на яких побудовано переважну кількість сучасних криптосистем, дозволяє стверджувати, що найбільш швидкими та ефективними є криві у формі Едвардса. При цьому відсутність національного стандарту, який би визначав механізм інкапсуляції ключа призводить до **постановки задачі**, яка полягає в стандартизації відповідного алгоритму. У проекті нового стандарту України авторами пропонується застосування скручених кривих Едвардса. **Мета** досліджень полягає в обґрунтуванні стійкості запропонованого алгоритму інкапсуляції (асиметричного шифрування) ключа або будь-якого короткого повідомлення, що використовує скручені криві Едвардса над простим полем.

Основні положення. Авторами запропоновано наступний *алгоритм обчислення шифротексту. Вхідними даними алгоритму є* загальні параметри алгоритму шифрування; відкритий ключ шифрування Q; повідомлення M фіксованої довжини; ідентифікатор iH функції ґешування H. *Вихідими даними алгоритму* є шифротекст $C=(r,t)$ (пара елементів з F_p) або повідомлення про помилку. *Алгоритм зашифрування:*

1. Обчислити значення $H(M)$, створити $M'=iH \parallel H(M) \parallel M$ і перевести його в $m'\in F_p$.

2. Обчислити точку $R=eP=(x_R,y_R)$ кривої. Встановити $r=x_R$.

3. Обчислити точку $T=eQ=(x_T,y_T)$ кривої.

4. Обчислити $t=x_R\cdot m' \bmod p$.

Результатом роботи алгоритму є шифротекст $C=(r,t)$.

Для *розшифрування повідомлення* використовуються наступні перетворення. Вхідними даними алгоритму розшифрування є загальні параметри системи шифрування; таємний ключ S шифрування; шифротекст $C=(r,t)$; ідентифікатор iH функції ґешування H. *Результатом виконання алгоритму* є розшифроване повідомлення M або повідомлення про помилку. Алгоритм розшифрування:

1. Обчислити елемент y поля F_p як $y=\left(\left(1-r^2\right)\left(a-dr^2\right)^{-1}\right)^{1/2}$. Встановити $R=(r,y)$.

2. Обчислити точку $T=(x_T,y_T)$ як $T=sR$. Встановити $t=x_T$.

3. Обчислити елемент $u=s\cdot t^{-1} \bmod p$ і перетворити на бітовий рядок U

4. З U виділити M і перевірити рівність отриманого та обчисленого значень $H(M)$.

Результатом алгоритму розшифрування є повідомлення M або повідомлення про помилку. **Висновок.** На основі аналізу різних методів інкапсуляції ключа було запропоновано до стандартизації розроблений авторами алгоритм, з використанням скручених кривих Едвардса. Для наведеного алгоритму вперше доведено, що задача дешифрування повідомлення зводиться до задачі Діффі-Хелмана, в той час як задача відновлення таємного ключа шифрування зводиться до задачі дискретного логарифмування в групі точок еліптичної кривої.

Білан А.М. (ВІТІ)
к.т.н Жук О.В. (ВІТІ)
Стемпковська Я.А. (ВІТІ)
Дука О.В. (ВІТІ)

КЛАСИФІКАЦІЯ КІБЕРЗЛОЧИНІВ У СУЧАСНИХ УМОВАХ РОЗВИТКУ КІБЕРПРОСТОРУ

Хвиля інформатизації накрила нашу країну. Суспільство поставило собі на службу телекомунікації й глобальні комп'ютерні мережі, не передбачивши, які можливості для зловживання створюють ці технології. Сьогодні жертвами злочинців, які безчинствують у віртуальному просторі, можуть стати не лише люди, але й держави. Безпека тисяч користувачів виявляється залежною від кількох злочинців.

Кіберзлочин − це суспільно небезпечне діяння, за яке установлюється кримінальна відповідальність (кібератаки, інші традиційні злочини, які вчиняються за допомогою сервісних можливостей та інформаційних ресурсів інформаційно-телекомунікаційних систем (ІТС). Особливостями проявів кіберзлочинів у кіберпросторі є: низькі затрати на реалізацію кіберзлочинів; зміни пріоритетів у діяльності злочинців − зміщення в кіберпростір, завоювання та утримання інформаційної переваги;ускладнення виявлення початку кіберзлочинів; відсутність статусу традиційних державних кордонів, що сприяє здійсненню кіберзлочинів.

На сьогодні відомо кілька класифікацій кіберзлочинів. Згідно з класифікацією, що була запропонована на рівні ООН (X Конгрес), усі кіберзлочини можна розділити на такі, що здійснюються проти ІТС (кіберзлочини у вузькому розумінні) й за допомогою ІТС (кіберзлочини в широкому розумінні).

Кіберзлочини, які визначені ратифікованою Україною Конвенцією про кіберзлочинність, поділяються на:

− правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем;

− правопорушення, пов'язані з комп'ютерами;

− правопорушення, пов'язані з дитячою порнографією;

− правопорушення, пов'язані з порушенням авторських та суміжних прав.

Рішенням Генерального секретаріату Інтерполу визначені способи учинення кіберзлочинів, які розкривають суть технологій: несанкціонованого доступу і перехоплення; зміни комп'ютерних даних; комп'ютерного шахрайства; незаконного копіювання; комп'ютерного саботажу; інших комп'ютерних злочинів.

Звісно, ця кодифікація спрощує проблему визначення професійних компетенцій фахівців із розслідування кіберзлочинів.

Натомість, класифікація кіберзлочинів відповідно до розділу XVI Кримінального кодексу України (злочини у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку) визначає злочини у вузькому розумінні (комп'ютерні інциденти), а також додаткові суспільно небезпечні діяння, що створюють передумови до здійснення комп'ютерних інцидентів та несанкціонованого збуту і розповсюдження інформації з обмеженим доступом.

Можливі шляхи вирішення проблеми протидії кіберзлочинам:

− створення відповідних органів управління та структурних підрозділів як на державному рівні, так і в Збройних силах України;

− удосконалення законодавчої та нормативно-правової бази з питань використання й захисту кіберпростору, протидії кіберзлочинам;

− організація підготовки відповідних спеціалістів;

− застосування сертифікованих комплексних систем захисту інформації в інформаційно-телекомунікаційних системах і мережах, які перешкоджають здійсненню кіберзлочину та сигналізують про спробу несанкціонованого доступу до інформації.

к.е.н. Білаш О.В. (НАСВ)
к.ф.-м.н. Глова Т.Я. (НАСВ)
к.ф.-м.н. Сорокатий М.І. (НАСВ)

ВДОСКОНАЛЕННЯ ПІДГОТОВКИ ВІЙСЬКОВИХ ФАХІВЦІВ НА ОСНОВІ ІНТЕНСИФІКАЦІЇ ПРАКТИЧНОГО ЗАНЯТТЯ

Актуальність. Військова освіта – це основа формування сильної армії та підготовки професійно-грамотних військових фахівців. Система воєнної освіти – складова частина державної системи освіти України, призначена для підготовки військових спеціалістів усіх освітньо-кваліфікаційних рівнів. Керівництво системою військової освіти здійснює Департамент військової освіти та науки, який є структурним підрозділом центрального апарату Міністерства оборони України.

Кожного року у системі військової освіти відбуваються зміни, які викликані низкою чинників, зокрема, змінами завдань та структури Збройних сил, розвитком озброєння та військової техніки, новими вимогами щодо спеціалізації та кваліфікації офіцерського складу, тощо. На нашу думку, система військової освіти повинна бути спрямована на забезпечення: неперервного оновлення вмінь та навичок, які отримують курсанти під час навчання; мобільності курсантів і викладачів; розробки і реалізації програм підготовки військових фахівців, попит на яких є найбільшим. Отримання якісної військової освіти є актуальною проблемою в зв'язку з військовими діями на сході Україні та необхідністю швидкого відновлення обороноздатності країни.

Мета. Проблемами покращення освітнього процесу загалом і якості надання освітніх послуг займалися такі науковці, як Ю.Н.Бараш, Я.Я.Болюбаш, К.М.Левківський, В.Мандрагеля, А.М. Москаленко, В.Л. Гуло, О.Г. Шаталова та інші. Проте, не зважаючи на велику кількість публікацій щодо даної тематики вона не досягнула своєї завершеності і тому проблема вдосконалення підготовки військових фахівців потребує подальшого дослідження.

Основні положення. У сучасний період є різні підходи у проведенні практичних занять у вищих військових закладах. Ми погоджуємося з думкою, що у навчанні важливий кожний курсант і його особистий попередній досвід. Окрім того, курсанти краще розуміють і сприймають той матеріал, який є наближеним до реального життя, можна буде використати у майбутньому та подається у формі не завчених книжних фраз. Важливу роль у сприйнятті матеріалу відіграють уміння викладача щодо: організації процесу навчання; формування зв'язку між їх спеціалізацією та дисципліною викладання; створення комфортного психологічного середовища для навчання, коли кожний курсант відчуватиме свою важливість та повагу від оточуючих; залучення курсанта до обговорення проблеми.

Варто зазначити, що розвиток сучасної військової освіти відбувається в напрямі компетентнісного підходу, сутність якого полягає у спрямованості освітнього процесу на формування та розвиток ключових і предметних компетенцій особистості. Таким чином, усі підходи до навчання є особистісно-орієнтованим, оскільки стосується особистості курсанта й може бути реалізованим і перевіреним тільки в процесі виконання конкретним курсантом певного комплексу дій. Такий підхід є найбільш ефективним, адже він базується на виявленні особливостей особистості і навчання курсанта за напрямком здійснюється відповідно до проведеного аналізу.

Програма навчання для курсантів вищих військових навчальних закладів включає вивчення загальних (базових) дисциплін та спеціалізованих військових, ґрунтовне вивчення та засвоєння яких є необхідним для отримання якісної військової освіти і підготовки висококваліфікованих військових фахівців.

В Україні існує низка перепон, які заважають розвитку військової освіти та вдосконаленню підготовки військових фахівців. На нашу думку, їх доцільно структурувати на зовнішні (до них відносимо військовий конфлікт, недосконаліть законодавства у цій

сфері, зменшення кількості населення, низький рівень фінансування) та внутрішні (формування груп курсантів різного рівня знань, посередні програми навчання, низький рівень підготовки вступників, зменшення кількості годин на викладання дисциплін).

Вагомим чинником вдосконалення підготовки військових фахівцівє запровадження ефективної методики викладання практичних занять, на яких засвоюється 75 % лекційного матеріалу. У Національній академії сухопутних військ імені гетьмана Петра Сагайдачного на кафедрі інженерної механіки використовують нову методику навчання, яка передбачає проведення та поділ кожного практичного заняття на такі етапи: ознайомчий, спрямований на актуалізацію знань курсантів, що пов'язані з темою, яка обговорюється та виявлення індивідуальних труднощів і прогалин в знаннях, усвідомлення та формулювання індивідуальних цілей навчальної діяльності;тематичний, на якому відбувається подання та сприйняття нової теми; підсумковий, який передбачає систематизацію і оцінювання отриманої інформації, формулювання нових запитань, закріплення почутого матеріалу. На цьому етапі доцільно поєднувати індивідуальну та групову роботи.

На нашу думку, одними із найважливіших складових навчального процесу, який вдосконалює підготовку військових фахівців є контроль та оцінка знань курсантів. Контроль є чинником, який демократизує, інтенсифікує та диференціює навчальний процес. Контроль проводиться протягом усіх етапів проведення практичного заняття та подальшого засвоєння матеріалу. Методами контролю, які використовуються при викладанні дисциплін "Вища математика" є: систематичне спостереження за навчальною роботою курсантів; усне опитування; написання контрольних робіт; виконання різноманітних задач і прикладів; проведення екзамену. Однак, перераховані вище методи є суб'єктивними, в зв'язку з чим доцільно ще проводити зовнішній контроль успішності курсантів у засвоєнні матеріалу, який базувався би на єдиній для всіх технології оцінювання. Ми вважаємо, що одним із дієвих засобів визначення якості освіти є проведення тестового опитування.

У більшості ВВНЗ у групах є курсанти, які мають різні базові знання та уміння, що також ускладнює процес засвоєння матеріалу, адже у кожного курсанта є свій період сприйняття та розуміння нової інформації. Ми вважаємо, що цю проблему можна вирішити шляхом групування курсантів за їх рівнем знань. Так, наприклад, одна група на кожній спеціальності повинна складатися із курсантів, які отримали найвищий бал при вступі; інші групи повинні сформуватися з решти курсантів, але таким чином, щоб кожна група складалася із однакової кількості курсантів з середнім і низьким рівнем знань. На нашу думку, такий розподіл допоможе приділяти більше уваги проблемним питанням у першій групі і швидше виявляти недоліки та упущення у навчанні в курсантів у рештах груп.

Ще однією запорукою підготовки військових фахівців є правильне формування програм навчання, які повинні узгоджуватися та взаємно доповнюватися, утворивши цілісну систему. Викладання тем з одного предмету має знаходити практичне (в окремих випадках – теоретичне) застосування, або бути логічним доповненням при вивченні тем іншого предмету. Цей процес підвищить мотивацію та зацікавленість курсантів до навчальних дисциплін. Також це розширить можливості викладачів, які будуть використовувати теоретичні знання курсантів з інших предметів, на практичних заняттях і допоможе курсантам швидше та ефективніше засвоювати новий матеріал.

Висновок. Отже, у системі військової освіти відбуваються постійні зміни з урахуванням досвіду зарубіжних країн та вітчизняних тенденцій. Проте, на нашу думку, незважаючи на значні нововведення, для удосконалення якості військової освіти необхідно: модернізовувати матеріально-технічні бази та інформаційно-методичне забезпечення освітнього процесу; вдосконалити програми військової підготовки; забезпечити ВВНЗ сучасними інформаційними системами. Ми вважаємо, що для вдосконалення підготовки військових фахівців необхідно здійснювати такі заходи: удосконалити відбір та здійснювати комплектування груп за рівнем знань курсантів; проводити практичні заняття на основі інтенсифікації практичного заняття та індивідуального підходу до кожного курсанта; здійснювати систематичний контроль за рівнем засвоєння курсантами нового матеріалу.

к.пед.н. Бірюков П.В. (ВІТІ)

ДОСВІД НАВЧАННЯ ВІЙСЬКОВИХ ФАХІВЦІВ США У СИНТЕТИЧНОМУ ВІРТУАЛЬНОМУ СЕРЕДОВИЩІ

США та провідні країни світу акцентують увагу на підготовці військових фахівців із застосуванням різного роду тренажерних систем та засобів імітаційного моделювання сучасного загальновійськового бою. Це зумовлено потребою скоротити витрати на проведення тактичних, тактико-спеціальних та інших навчань на полігонах у реальному часі, підвищити якість підготовки військовослужбовців за рахунок відпрацювання реалістичних сценаріїв бойових операцій, які не можливо відтворити в реальному середовищі, більш раціонально та ретельно готувати екіпажі (розрахунки) перед їх обкаткою на полігонах та стрільбищах. Такий підхід в організації освітнього процесу військових фахівців є вкрай актуальним для нашої країни в контексті триваючого збройного протистояння підрозділів Збройних Сил України з російськими окупаційними військами.

Метою статті є вивчення досвіду запровадження систем імітаційного моделювання у підготовці військових фахівців США на прикладі співпраці з компанією Raytheon, яка спеціалізується на високотехнологічних розробках в галузі оборони та кібернетики.

На наш погляд, корисним є досвід навчання американських військовослужбовців, екіпажів, підрозділів у межах програми Global Training Solutions, запровадженої компанією Raytheon. Ця компанія приступила до оснащення навчального центру армії США, розташованого у місті Форт-Полк, штат Луїзіана, високотехнологічними можливостями моделювання. Навчальний центр має назву Шугхарт-Гордон на честь двох військовослужбовців – одержувачів медалі Пошани, вбитих під час спроби врятувати солдатів зі збитого вертольоту „Чорний яструб" у сомалійському місті Могадішо. Підрозділи американської армії зі всіх куточків країни в навчальному центрі вже більше 20 років беруть участь у двотижневих навчальних вправах, відтворюючих бій до найдрібніших деталей. Армія тренується на більшості сценаріїв, заснованих на реальних військових операціях у світі.

Raytheon вдосконалює, розширює та модернізує системи, що керують реалістичними бойовими моделюваннями в Центрі військових операцій США в умовах урбанізованої місцевості. Форт Полк є домом для першого спільного цифрового регіонального навчального центру, який завдяки Raytheon оснащений:

– 700 мережевими інфрачервоними моделями камер високої чіткості з потрійною роздільною здатністю та можливістю записувати відео та аудіо в будь-якій кімнаті кожної будівлі;

– комп'ютерами, відеореєстраторами, дисплеями та системами спеціальних ефектів, мережевим обладнанням;

– системою контролю спеціальних ефектів: вибухи на даху та кулі, імітатори зброї, звукові ефекти та звичайні функції, такі як освітлення та замки. Солдати можуть почути, як дитина плаче в одній кімнаті, радіо грає музику в іншій і бійці ворожої сторони шепочуть про напад. Система також створюватиме аромати - від стічних вод до екзотичних спецій - які роблять сценарії більш реалістичними.

Інтегрована система лазерного випромінювання Multiple Integrated Laser Engagement System (далі – MILES) – високотехнологічна установка „лазерної мітки" відстежує, як і коли учасники вправ та їх обладнання потрапляють у зону вогню противника. Після кожної тренувальної вправи з командирами підрозділів проводиться підсумковий розбір. Одне із завдань тренінгу: навчити війська ігнорувати відволікаючі фактори та налаштувати бойове мислення. Наприклад, бійці, як правило, схильні до приємних запахів, уникаючи ділянок, які смердять як каналізація, проте їм потрібно змінити цей спосіб мислення, тому що там, як правило, ховається ворог.

Жодний сценарій не є справді реальним без людського елемента, у місті є акторський склад цивільних осіб, які виконують ролі місцевих жителів, власників магазинів, міських чиновників, журналістів, змішуючись із військами та ускладнюючи обстановку.

Армія США будує синтетичне поле битви, щоб можна було приєднатися до навчання в прямому ефірі. У доповненій реальності, створеному комп'ютером або реальним світом, сенсорний контент розміщується над зором солдата на реальне середовище.

За допомогою Fortnite можна зіграти бойову роль проти інших учасників у всьому світі незалежно від платформи відеозв'язку, що використовується: PS4, Xbox One, Nintendo Switch, Mac, ПК або смартфон. Це називається кросплатформна гра або кроссплей. Подібний віртуальний світ Fortnite дозволяє таку взаємодію.

Американська армія зацікавлена в такому підході, вивчаючи додаткові концепції та технології для підготовки своїх підрозділів. Сервіс хоче використовувати віртуальну та ігрову технологію, пристосовану для військових програм, спираючись на загальний набір даних у модульній архітектурі відкритих систем. Завдяки обладнанню Синтетичне навчальне середовище Synthetic Training Environment (далі - STE) буде доступною функцією швидкого підключення військовослужбовців. Завдяки STE збройним силам не доведеться мати справу з логістикою планування та переміщення військовослужбовців до навчальних центрів. Вони можуть тренуватися на своїх домашніх пристроях з мінімальними накладними витратами або навіть під час дислокації.

Хоча армія США проводить загальновійськові синтетичні тренування у складних, оперативних умовах, використовуючи свої віртуальні тренажери для вертольотів та танків, імітаційне моделювання для командирів та штабів, їй не вистачає загального синтетичного середовища. Вона використовує власні системи, які мають складнощі в сумісності. Поєднання різних систем для тренувань вимагає часу та витрат. Цю проблему успішно вирішує STE.

STE підходить для тренувань у повітрі, на суші, на морі, у космосі та кіберпросторі, використовуючи віртуальне та конструктивне середовище, яке буде поєднуватися з реальними навчальними вправами. Реальна підготовка завжди буде завершальним випробуванням до того, як армія відправить підрозділи в бій. Але перед реальними випробуваннями, вони навчатимуться у віртуальному та конструктивному світі. Солдати можуть репетирувати місію декілька разів, не ризикуючи життям або кінцівкою. Вони можуть практикувати надзвичайні ситуації та критично важливі завдання, які не можна безпечно повторювати під час тренувань у реальному світі, як, наприклад, вихід з ладу двигуна на справжньому літальному апарату.

Армія США має за мету створити єдиний реконфігуруваний віртуальний колективний тренувальний майданчик для бронетехніки, на базі танку M1 Abrams, бойової машини M2 Bradley, M1126 Stryker або бойових машин нового покоління. У разі необхідності для солдата система відшукає віртуального тренера, який дозволить тим, хто навчається, приймати дії разом або самостійно. Солдати будуть носити „інтегровану систему візуальної збільшення", яка використовує захисні окуляри Microsoft HoloLens. Віртуальне чи синтетичне середовище потребує зв'язку з реальним середовищем для тренувань. Ви не можете відтворити перебування в бруді та грязі, потінні та недосипанні.

Raytheon працює з віртуальними моделюваннями STE Soldier and Squad та STE Live Force on-Force. Нові технології дозволять навчальній системі використовувати штучний інтелект для визначення рівня майстерності тих, хто навчається, і автоматично пропускати те, що вони вже знають, при цьому створювати складні варіативні ситуації.

Таким чином, досвід підготовки військових фахівців США у синтетичному навчальному середовищі, поєднання імітаційного модельованого навчання з реальними випробуваннями, напрями створення віртуальних колективних майданчиків для навчання навичкам управління озброєнням та військовою технікою, є корисним у площині створення і удосконалення тренажерних засобів на базі симуляційних комп'ютерних технологій в Україні.

Бовда В.Е. (НТУУ „КПІ”)

ПЕТРІ-ОБ’ЄКТНА МОДЕЛЬ ТРАНСПОРТНИХ ПЕРЕВЕЗЕНЬ МАТЕРІАЛЬНИХ ЗАСОБІВ У ВІЙСЬКОВИХ ПІДРОЗДІЛАХ

Величезні поставки військових ресурсів по всій країні вимагають великих витрат на перевезення. Планування маршрутів перевезень, які б забезпечили вчасну доставку та економію загальних витрат на доставку становить складну задачу для військового логіста. В даний час проблеми розвитку транспортної інфраструктури, вдосконалення засобів логістики, інтелектуалізація програмних засобів та інформаційних технологій супроводу та підтримки прийняття рішень на транспорті набувають сьогодні першочергового значення. Тому на даний момент існує необхідність у створенні програмного забезпечення для військових логістів, що дозволяло би швидко та ефективно планувати поставки військових ресурсів, які б забезпечували вчасну доставку та економили витрати на перевезення.

Існуючі алгоритми автоматизованого планування вантажоперевезень не завжди відповідають сучасним вимогам, або вимагають залучення занадто великих технічних ресурсів. Розробка нових алгоритмів може дозволити скоротити час пошуку рішень в задачах великої розмірності, і водночас підвищити якість одержуваних рішень за рахунок розробки нової архітектури пошуку. Об’єктом дослідження є транспортно-логістичні процеси, що відбуваються при забезпечені військових підрозділів. Метою дослідження є розробка Петрі-об’єктної моделі транспортних перевезень матеріальних засобів у військових підрозділах.

Для рішення цієї задачі використовується генетичний алгоритм, де в процесі моделювання отримаємо кращі рішення, які представляють собою необхідну кількість машин у кожному складі та маршрути розвезення військового устаткування для кожної машини з одночасним рішенням по витратах палива та загального часу затримки [1].

У запропонованій моделі військове устаткування та ресурси (транспортні засоби) для доставки товарів представляються у вигляді позицій мереж Петрі. Шляхи між військовими складами та частинами представляються у вигляді переходів мереж Петрі. Ці переходи мають пріоритет, який буде геном у генетичному алгоритмі. Найменша мережа Петрі представляє собою транспортний засіб, який рухається між пунктами призначення, які потребують певного військового устаткування. Транспортний засіб рухається між пунктами в залежності від пріоритетів переходів і доставляє військове устаткування у ці пункти. Оскільки транспортний засіб має обмежену вантажопідйомність та обмеження на одне пересування з кожної пари пунктів, то врешті-решт транспортний засіб повернеться на базу для завантаження нових замовлень. Кожен склад може мати в своєму розпорядженні декілька транспортних засобів, а значить, мережі Петрі транспортних засобів мають спільне військове устаткування для виконання замовлень.

В результаті дослідження створено Петрі-об’єктну модель транспортних перевезень матеріальних засобів у військових підрозділах, де в якості цільової функції вибрано суму витрат пального та сумарну затримку доставок замовлень. Описано алгоритм оптимізації рішення транспортної задачі, який дозволяє зменшити загальний час затримки доставки військового устаткування та зменшити витрати пального. Перевагою моделі є її стохастичність, що дозволяє моделювати невизначені процеси, що в свою чергу, наближає моделювання транспортних перевезень матеріальних засобів до реальних значень. Модель дозволяє проводити моделювання транспортних перевезень у складних багаторівневих ієрархічних системах.

ЛІТЕРАТУРА

1. Бовда В.Е. Петрі-об’єктне моделювання транспортних перевезень матеріальних засобів у військових підрозділах / В.Е. Бовда, Е.М. Бовда, І.В. Стеценко – Київ: Збірник наукових праць Військового інституту телекомунікацій та інформатизації. – Випуск № 3. 2019, С. 6 – 15.

к.т.н. Бовда Е.М. (ВІТІ)

БОЙОВЕ ЗАСТОСУВАННЯ ПІДРОЗДІЛІВ ЗВ'ЯЗКУ З УРАХУВАННЯМ ДОСВІДУ ОПЕРАЦІЇ ОБ'ЄДНАНИХ СИЛ

В останні роки, з досвіду операції об'єднаних сил, бойове застосування підрозділів зв'язку зазнало значних змін – це пов'язано з:

1. Збільшенням числа родів зв'язку, які використовуються в організації військового зв'язку – транкінговий, радіорелейний, радіо та супутниковий зв'язок, засоби спецзв'язку та фельєгерсько-поштовий зв'язок.

Транкінговий, радіо та супутниковий зв'язок перетворились на основні роди зв'язку в тактичній ланці управління, а в оперативній та оперативно-тактичній ланці знайшло використання радіозв'язку з ППРЧ в КХ діапазоні. Супутниковий зв'язок є не тільки в механізованому батальйоні, а також на окремих ротних та взводних опорних пунктах.

2. Використанням комутаторів П-193, П-194 та телефонів ТА-57 разом з ТК-1 в тактичній ланці управління.

3. Переоснащенням апаратних тактичного та оперативно-тактичного рівня на радіостанції *Harris*, *Motorola*, *Aselsan*, станції супутникового зв'язку та засоби спецзв'язку.

4. Доведенням до взводного опорного пункту проводового зв'язку.

5. Використанням комплексної апаратної зв'язку (КАЗ) та іншої цифрової техніки, що дозволило значно скоротити кількість апаратних на вузлах зв'язку пунктів управління (ВЗ ПУ) вищих ланок управління.

6. Отриманням КАЗ промислового виробництва.

Перевагами використання КАЗ є:

а) збільшення числа автоматизованих робочих місць (АРМ) посадових осіб в локальній обчислювальній мережі (ЛОМ) ВЗ ПУ вищих ланок управління в залежності від завдань;

б) підвищення мобільності ВЗ ПУ за рахунок зменшення числа апаратних зв'язку;

в) підвищення пропускної здатності мережі за рахунок тактико-технічних характеристик апаратури, що розміщена в апаратних;

г) збільшення розвідзахищеності системи зв'язку (використання ППРЧ);

д) зменшення площі розгортання ВЗ ПУ на місцевості;

е) зменшення кількості центрів вузла зв'язку – КАЗ виконує функції трьох центрів (каналоутворення, телефонного, телеграфного (документального)) та називається центром інформаційних систем;

є) збільшення можливостей КАЗ за рахунок нарощування апаратури в телекомунікаційних стійках під завдання, що ставляться.

7. Використанням модульного принципу розгортання вузла зв'язку із збільшенням числа модулів для виконання більшого об'єму завдань за потреби.

8. Використанням системи відеоконференцзв'язку в стаціонарній компоненті до тактичної ланки.

9. Підключенням до системи електронного документообігу стаціонарної та польової компонент.

10. Підвищенням рівня кібербезпеки мереж Збройних сил України.

11. Створенням у Збройних силах України наземних мобільних станцій супутникового зв'язку.

Відбулися зміни в самій системі зв'язку в зоні операції об'єднаних сил (ООС). Телекомунікаційна мережа загального користування активно використовується для прив'язки мобільними засобами за допомогою малогабаритних станцій широкосмугового доступу типу нового покоління.

Разом з тим, малогабаритні станції широкосмугового доступу активно замінюються на радіорелейну станції вітчизняного виробництва Р-402.

Польова компонента системи зв'язку будується на лініях прив'язки ВЗ ПУ до ТМЗК та на лініях супутникового зв'язку між ПУ.

В ході управління підрозділами в ООС застосовуються наступні види зв'язку:

1. Телефонний відкритий (IP-ТФ), який організований за допомогою цифрових автоматизованих телефонних станцій (ЦАТС), призначених для ведення відкритих телефонних переговорів між абонентами вузлів зв'язку пунктів управління ЗС України.

2. Телефонний зв'язок для ведення переговорів з обмеженим доступом, де встановлено відповідне обладнання.

3. Передача даних за допомогою автоматизованої системи управління (АСУ ПД) „Дніпро".

4. Відеотелефонний зв'язок.

Сьогодні телекомунікаційна система ЗС України постійно готова, достатньо ефективна, стійка, мобільна, розвідзахищена, з відповідною пропускною здатністю. Але цього не достатньо, тому робота щодо її вдосконалення триває.

Сучасні радіозасоби тактичної і оперативно-тактичної ланки управління вже надходять у війська та поступово заміняють транкінг. Для оснащення частин закуповують високотехнологічні цифрові радіостанції *Harris* та *Aselsan*. Вони стануть базовими для військ на коротких та ультракоротких хвилях.

Досить гостро стоїть питання кібернетичної безпеки.

Актуальним буде питання розгортання системи зв'язку ЗС України на нових цифрових засобах зв'язку.

Йдеться про сучасні засоби радіорелейного і тропосферного зв'язку, завадостійкі і компактні КХ-УКХ радіостанції українського та іноземного виробництва, нові КАЗ, КШМ і апаратні, кабельну систему і відеозв'язок, новітні засоби радіо та аеророзвідки, радіоелектронної боротьби.

Також триває робота по реалізації створення ефективної системи оперативного (бойового) управління, зв'язку, розвідки та спостереження ЗС України (*C4ISR*) та Єдиної інформаційної системи управління оборонними ресурсами.

Висновки

В цілому процес розгортання системи управління ЗС України відбувається поетапно з поступовим запровадженням стандартів НАТО (AJP-6 „Єдиній доктрині для систем зв'язку та інформаційних систем").

Нові принципи та підходи організації, використання зв'язку та інформаційних систем в сучасних умовах відбувається в ЗС України з урахуванням нового досвіду бойового застосування частин та підрозділів зв'язку, так і з огляду на вимоги базових документів, які визначають цілі нашої оборонної реформи, а саме:

переоснащення польової (мобільної) компоненти автоматизованою системою оперативного (бойового) управління, зв'язку, розвідки та спостереження (аналог *C4ISR*), впровадження цифрових засобів з високим рівнем завадостійкості та розвідзахищеності, які відповідають стандартам НАТО (створення нової архітектури мобільної компоненти тактичних мереж зв'язку у Збройних силах України – за аналогією WIN-T (Warfighter Information Network-Tactical) та створення телекомунікаційного комплексу оперативно-тактичної ланки управління – за аналогією Mobile Subscriber Equipment (MSE));

використання інтеграційної платформи *Delta* (власне спеціальне програмне забезпечення);

інтеграція волонтерських проектів автоматизації та наданих у рамках військово-технічної допомоги від уряду США;

запровадження досвіду організації зв'язку в умовах ведення бойових дій в практику військ;

втілення бойового досвіду в програми підготовки курсантів інституту.

к.т.н. Бойко О.В. (ВДА імені Є. Березняка)
к.т.н. Буяло О.В. (ВДА імені Є. Березняка)
к.т.н. Пилипчук В.В. (ВДА імені Є. Березняка)

МЕТОДИКА МОДИФІКАЦІЇ ОПЕРАЦІЙНОЇ СИСТЕМИ ANDROID НА МОБІЛЬНИХ ПРИСТРОЯХ ДЛЯ ЗАПОБІГАННЯ ПЕРЕДАЧІ СТАТИСТИЧНОЇ ІНФОРМАЦІЇ

Сучасні мобільні пристрої (МП) дають можливість виконувати ряд завдань, однак не забезпечують користувачів від потенційних загроз. Одна з цих загроз полягає в тому, що транснаціональні корпорації та компанії-виробники сучасної мобільної техніки можуть вести спостереження за користувачами за допомогаю вбудованого програмного забезпечення, яке під час доступу до мережі Інтернет передає різноманітні дані, так звану статистичну інформацію, на сервери компаній.

Це зменшує швидкодію МП через наявність залишкового програмного забезпечення, яке займає постійну та оперативну пам'ять, що негативно впливає на швидкість виконання завдань. Аналіз показує, що більшість МП (73 %) працює на базі ОС Android, тому постає потреба у модифікації операційної системи Android на мобільних пристрояї для запобігання передачі статистичної інформації виробнику та розробнику популярного програмного забезпечення.

Операційна система Android має відкритий вихідний код, і отже є доступною для будь-якого користувача, який може вносити зміни, доповнення, що значно полегшить налаштування мобільного пристрою. З урахуванням вищезазначеного розроблено методику модифікації операційної системи Android на мобільних пристроях, яка складається з трьох етапів: підготовчого, основного та кінцевого

Підготовчий етап включає вибір МП, підготовку робочого місця, отримання прошивки для обраного пристрою та підготовку МП до роботи. Другий основний етап методики найбільш трудомісткий, він потребує від виконавця уваги, базових знань системи Linux та зокрема її команд. Цей етап складається з операцій, спрямованих на усунення загроз і зменшення ризиків неконтрольованого витоку інформації з пристрою.

На цьому етапі здійснюється розпакування офіційної прошивки, \\ модифікація, запаковування прошивки та встановлення на МП.

Розпакування та запаковування прошивки здійснюється за допомогою встановленого спеціалізованого програмного забезпечення. Модифікація прошивки включає декілька етапів: підготовку програмного забезпечення в прошивці, видалення програмного забезпечення Google, видалення програмного забезпечення виробника та додаткові налаштування для блокування небажаних сервісів. виконання цих задач потрібно здійснити попередній аналіз програмного забезпечення в прошивці МП.

Третій етап методики найкоротший, проте також важливий. На цьому етапі відповідно до рекомендацій здійснюється перший запуск і налаштування модифікованої прошивки. Далі перевіряють працездатність прошивки та повертають офіційний засібу віднов лення (скидання) налаштувань у разі непередбачуваних обставин (наприклад, зараження вірусом) або небезпеки.

Для оцінки ефективності методики модифікації операційної системи Android на мобільних пристроях проведено експеримент, суть якого полягає в аналізі трафіку МП на прошивці без змін та з ними.

В результаті швидкість першого включення пристрою зросла на 34 %, швидкість перезавантаження пристрою – на 14 %, розмір прошивки зменшено на 35 %, а обсяг оперативної пам'яті – на 20%, що позитивно впливає на доступне місце на МП та на підвищення швидкості виконання завдань.

Бондаренко Л.О. (НЦЗІ ВІТІ)
Бондаренко О.Є. (НЦЗІ ВІТІ)
Бузаєва К.О. (НЦЗІ ВІТІ)
Руденко В.І. (НЦЗІ ВІТІ)

УПРАВЛІННЯ ТЕЛЕКОМУНІКАЦІЙНОЮ ІНФРАСТРУКТУРОЮ ЗБРОЙНИХ СИЛ УКРАЇНИ: СТАН, ЗАДАЧІ, ПІДХОДИ І ПЕРСПЕКТИВИ

Актуальність. На підставі аналізу побудови системи управління телекомунікаційною інфраструктурою (СУІ) ЗС України, а також оцінки практичної роботи органів управління і чергових змін ІТВ можливо зробити висновок про те, що завдання організаційного і технологічного управління телекомунікаційною інфраструктурою і її елементами проводяться в неавтоматизованому режимі.

Постановка задачі. Під управлінням телекомунікаційною інфраструктурою розуміють цілеспрямовані дії, що пов'язані з плануванням, розгортанням (побудовою) та експлуатацією мереж, що роблять більш ефективним використання їх ресурсів. Тому основними завданнями системи управління телекомунікаційною інфраструктурою протягом усього життєвого
циклу є:

розгортання і введення в експлуатацію телекомунікаційних мереж;

здійснення процесу експлуатації;

розвиток мереж.

СУІ повинна представляти собою єдину систему обміну інформацією через керуючі додатки, автоматизацію завдань управління пристроями, огляд стану і продуктивності мережі, а також виявлення та визначення мережевих несправностей.

Метою роботи є визначення існуючого стану управлінням телекомунікаційною інфраструктурою Збройних сил України,основні задачі, що до неї висуваються, підходи та перспективи.

Основні положення. Одним з основних стандартів при побудові систем управління різнорідними територіально розподіленими телекомунікаційними мережами є концепція телекомунікаційної керуючої мережі Telecommunication Management Network (TMN), що запропонована Міжнародним союзом електрозв'язку (ITU). Концепція TMN викладена в рекомендаціях серії M.3xxx і заснована на базових принципах управління відкритими системами, які визначені стандартом ISO 7498-4.

СУІ, незалежно від характеристик об'єктів управління, повинна виконувати ряд функцій, які визначені міжнародними стандартами, узагальнюючими досвід застосування систем управління телекомунікаціями, а саме рекомендації ITU-T X.700 і близький до них стандарт ISO 7498-4, які ділять завдання системи управління на п'ять функціональних груп:

управління конфігурацією мережі та ім'ям;

обробка помилок;

аналіз продуктивності та надійності;

управління безпекою;

облік роботи мережі.

Вибір СУІ з урахуванням її адаптації під конкретну телекомунікаційну інфраструктуру – складна багатокритеріальна задача, тому вибір і побудова системи управління повинні починатися з розробки технічного завдання на СУІ.

Структура СУІ повинна являти собою апаратно-програмні комплекси, які призначені для моніторингу стану, аналізу працездатності та управління апаратними та програмними засобами телекомунікаційних мереж.

СУІ повинна здійснювати:

моніторинг і аналіз функціонування програмно-технічних засобів функціональних та технологічних підсистем;

організаційне та автоматизоване управління функціонуванням програмно-технічних засобів функціональних та технологічних підсистем.

СУІ повинна забезпечувати:

інтеграцію засобів адміністрування функціональних і технологічних підсистем;

контроль параметрів функціонування апаратного та програмного забезпечення серверів і робочих станцій телекомунікаційних мереж;

аналіз даних про функціонування підсистем і розподілених додатків;

накопичення, аналіз і відображення результатів контролю стану і працездатності елементів телекомунікаційних мереж;

своєчасне виявлення, локалізацію і управління усунення несправностей;

прогнозування критичних станів системи та запобігання виникненню відмов у роботі елементів телекомунікаційних мереж на ранній стадії;

вироблення команд і сигналів управління технічними і програмними засобами підсистем в автоматичному і ручному режимах для прийняття рішення системним адміністратором;

оптимізацію планування завдань обслуговування системи з урахуванням завантаженості ресурсів телекомунікаційних мереж;

оптимальний розподіл загальних обчислювальних і комунікаційних ресурсів з урахуванням їх значущості в системі управління військами (силами) і зброєю;

автоматизацію планування діяльності персоналу з управління функціонуванням при технічному обслуговуванні та регламентних роботах;

реєстрацію та документування подій в телекомунікаційних мережах, дій адміністраторів з управління функціональними і технологічними підсистемами.

При реалізації зазначених функцій в СУІ доцільно використовувати:

способи моніторингу – активний, пасивний або їх комбінацію;

методи управління – централізований, децентралізований або їх комбінацію.

В основі СУІ повинна лежати схема взаємодії агента з менеджером. Спеціалізоване програмне забезпечення СУІ повинне складатися з трьох окремих програмних компонентів - серверного, клієнтського і агентського програмних модулів, які забезпечують формування інформації для прийняття управлінських рішень.

На основі цієї схеми можуть бути побудовані системи практично будь-якої складності з великою кількістю агентів та менеджерів різного типу.

Підготовлена інформація в СУІ формується за результатами моніторингу елементів мереж за напрямками: моніторинг послуг, системний моніторинг, ресурсний моніторинг, апаратний моніторинг, моніторинг геопозиціонування інфраструктури, моніторинг витрат, моніторинг ефективності, пооперaційний моніторинг.

Завдання системи моніторингу СУІ, критерії та показники її роботи повинні обиратися методом експертної оцінки, в залежності від місця і ролі телекомунікаційної мережі в системі управління військами (силами) та зброєю.

Висновок. Таким чином, СУІ повинна розроблятися для досягнення кінцевої мети:

підготовка інформації для прийняття управлінських рішень;

доведення необхідної інформації до посадових осіб, які приймають рішення щодо управління системою;

забезпечення необхідної готовності телекомунікаційних мереж з Кг≥Кг доп;

забезпечення заданої якості послуг з інтегрованою оцінкою не нижче встановленої;

оптимізації використання та збільшення реального завантаження телекомунікаційних ресурсів;

перехід від ідеології контролю SLA до ідеології управління SLA;

повний перехід на управління ризиками.

к.т.н. Борисов І.В. (ВІТІ)
Березанський Д.О. (А1906)
Петрова Д.В. (ВІТІ)

ОБҐРУНТУВАННЯ І СУТНІСТЬ МЕТОДИКИ ОБРОБКИ СИГНАЛІВ В СИСТЕМІ MIMO ПРИ ВПЛИВІ НАВМИСНИХ ЗАВАД

Негативний вплив навмисних завад в системах радіозв'язку з MIMO може бути значно послаблений за рахунок застосування адаптивних алгоритмів формування та обробки сигналів з використанням адаптивних антенних решіток.

Сутність розробленої в даному розділі методики полягає в адаптивному управлінні параметрами засобів радіозв'язку з MIMO в залежності від стану каналу зв'язку, за критерієм максимуму коефіцієнту використання потужності сигналу при виконанні обмежень на ймовірність бітової помилки.

Постановка завдання.

Задано: параметри системи MIMO і каналу зв'язку Ф = {φ_i}, $i = \overline{1,8}$, де $\varphi_1 \ldots \varphi_8$ – кількість передавальних та приймальних антен, кількість ітерацій, розмірність ансамблю сигналів, тривалість кадру на виході демодулятора L^*, тривалість кадру на виході декодера L, швидкість коригувального коду, величина кодової відстані.

Необхідно: визначити параметри і режим роботи MIMO-системи, які максимізують енергетичну ефективність засобу радіозв'язку при виконанні обмеження на значення ймовірності помилкового приймання сигналів.*Обмеження*: $\tau_{гр} \le \tau_{кор}$, де $\tau_{гр}$ – тривалість групи символів, $\tau_{кор}$ – час кореляції завмирань; розмірність ансамблю сигналів $2 \le M \le 64$; кількість передавальних антен $M_t \le 8$; кількість приймальних антен $M_r \le 8$; швидкість коригувального коду R = 0,5-0,9; ймовірність помилкового приймання сигналів $P_{пом} \le 10^{-3}$.

Допущення: канальна матриця **H** є постійною за час $\tau_{гр}$.

Завдання визначення значень параметрів системи MIMO при дії навмисних завад зводиться до типової оптимізаційної задачі. Система рівнянь для вирішення оптимізаційної задачі має вигляд:

$$\begin{cases} \beta_E = F_1(v_i, \Delta F, M, n, R, d, P_c) \to \max; \\ P_б = F_2(P_c, M, n, R, d, N_A) \le P_{б\,доп}, \end{cases} \quad (1)$$

де v_i – інформаційна швидкість, $P_б$ – ймовірність помилки на біт, n– довжина кодової комбінації, P_c– потужність сигналу, M – розмірність ансамблю сигналів, R – швидкість коригувального коду, $R = k/n$, k – кількість інформаційних біт в кодовій комбінації довжиною n, d– величина кодової відстані, ΔF – ширина спектра сигналу, де $P_б$ – ймовірність бітової помилки.

Розкриємо функціонали системи рівнянь (1). Ймовірність бітової помилки визначається як:

$$P_{пом} \approx \frac{1}{M} \sum_{k=1}^{M} \sum_{\substack{i=1 \\ k \ne i}}^{M} \frac{1}{2} \left[1 \quad \Phi\left(\sqrt{\frac{d_{ki}^2}{2G_0 + G_з}} \right) \right], \quad (2)$$

де $\Phi(x) = \frac{2}{\sqrt{2\pi}} \int_0^x e^{\left(-\frac{t^2}{2}\right)} dt$ – функція Крампа, $G_з$ – спектральна щільність навмисної завади, d_{ki} – відстань між сигналами з номерами k і i.

Швидкість передачі інформації визначається як:

$$\nu_{\text{і}} = \frac{B}{\tau_{\text{і}}} = \frac{M_t \cdot M_r \cdot \log_2 M}{\tau_{\text{і}}}, \qquad (3)$$

де B – кількість інформаційних біт, що передається за один радіоімпульс, $\tau_{\text{і}}$ – тривалість радіоімпульсу.

Таким чином, з виразу (3) видно, що значення швидкості передачі інформації залежить від значення тривалості радіоімпульсу.

Енергетична ефективність визначається, як

$$\beta_E = \nu_{\text{і}} / Q_{\Sigma}^2, \qquad (4)$$

Де $Q_{\Sigma}^2 = \frac{E_{\text{с}}}{G_0 + G_{\text{з}}}$ – відношення енергії сигналу до сумиспектральних щільностей потужностей білогогаусівського шуму та навмисної завади.

Методика обробки сигналів в приймальному тракті системи MIMO складається з наступних етапів.

Введення вихідних даних. Вводяться параметри системи MIMO і каналу зв'язку (блок 1) Ф = {φ_i}, $i = \overline{1,8}$, де $\varphi_1 \ldots \varphi_8$ – кількість передавальних та приймальних антен, кількість ітерацій, розмірність ансамблю сигналів, тривалість кадру на виході демодулятора L^*, тривалість кадру на виході декодера L, швидкість коригувального коду, величина кодової відстані.

Оцінка стану каналу зв'язку. Розробка і впровадження адаптивних методів інформаційного обміну вимагають створення ефективних процедур контролю та прогнозування стану каналів зв'язку і якості передачі інформації.

Визначення методу обробки сигналів в системі MIMO. В залежності від значення відношення сигнал/завада Q^2 в каналі, вибирається метод обробки сигналів.

Обробка сигналів в антенній решітці.

При низьких відношеннях сигнал/завада в каналі зв'язку $Q^2 \le Q_{\text{гр}}^2$ для забезпечення передачі інформації пропонується застосовувати адаптивну обробку просторово-часових сигналів на прийомі, що забезпечує максимізацію діаграми спрямованості приймальної антени на сигнал з максимальною потужністю і подавлення інших сигналів з меншими потужностями.

При цьому всі елементи антенної решітки діляться на блоки, кожний з яких містить у собі певну кількість антен. Число елементів у блоках n є незмінною величиною і залежить від загальної кількості елементів антени, і кількості просторових радіотрактів. Адаптація здійснюється за критерієм максимізації відношення сигнал/завада.

Оцінка прийнятого сигналу. Наступною операцією є оцінка переданих символів за одним із критеріїв. Результатом оцінки переданої матриці вектора символів є кілька паралельних потоків даних, які необхідно об'єднати для подальшої демодуляції.

Цю операцію виконує мультиплексор, який перетворює декілька послідовностей в одну.

Взагалі, даний метод перетворення сигналів є вертикальним просторовим мультиплексуванням, де операція мультиплексування виконується перед демодуляцією сигналу.

Розроблена методика полягає в тому, що при обробці сигналів в каналі з гранично низьким відношенням сигнал/завада вводиться додаткова процедура просторової фільтрації сигналів з урахуванням характеристик навмисних завад.

Бруяка Р.В. (ВІТІ)
Грохольський Я.М. (ВІТІ)

ВАРІАНТ МОДЕРНІЗАЦІЇ ТЕЛЕКОМУНІКАЦІЙНОГО КОМПЛЕКТУ ТИП-1

Дослідження пов’язана з необхідністю модернізації та розробки нових засобів зв’язку. Варіантом таких засобів зв’язку можуть слугувати телекомунікаційні комплекти тактичної ланки управління, які дають змогу поєднати можливості телефонних мереж та мережі передачі даних. **Мета.** Здійснити аналіз основних засобів побудови телефонного зв’язку та систем передачі даних тактичної ланки управління ЗСУ та представити варіанти модернізації. В даний час йде процес інтенсивного розвитку IP-телефонії, що об’єднує їх в єдину комунікаційну мережу, яка пропонує потужний і економічний засіб зв’язку. Рішення IP-телефонії комбінують голос і дані в одній мережі і пропонують дешеві міжнародні і міжміські дзвінки і цілий набір комунікаційних послуг будь-якому користувачеві. При побудові ж систем телефонного зв’язку тактичної ланки управління на відміну від традиційної телефонної мережі може використовуватися і система передачі даних. Створена ж система передачі даних в ЗС отримала назву АСУ „Дніпро”. У розв’язуваних завданнях з переведення системи зв’язку Збройних сил на цифрове телекомунікаційне обладнання найбільш складним завданням є переведення її польової компоненти. Відтак, багато компаній України проектує та виготовляє техніку для сектору безпеки та оборони, використовуючи потенціал власного проектного конструкторсько-технологічного бюро та збиральну лінію, оснащену високотехнологічним обладнанням. Це такі компанії як „Телекарт-прилад”, „Датагруп” та „Еверест Лімітед”. Кожен виготовлений зразок техніки проходить ретельну перевірку спеціалістами технічного контролю. Телекомунікаційний комплект ТИП-1 – польовий маршрутизатор тактичної ланки управління з підтримкою *VoIP* телефонії (далі – *ТК-1*), призначений для забезпечення відкритого телефонного зв’язку та передачі даних на блокпостах та взводних (ротних) опорних пунктах та є закінченим телекомунікаційним пристроєм. Технічно ТК-1 не є цільним пристроєм, елементи якого розпаяні на одній платі, і складається з 4х різних за функціональним призначенням пристроїв (маршрутизатор, комутатор, VoIP-шлюз та міні-комп’ютер), LCD дисплею та блоку живлення які з’єднані грубо між собою провідниками.

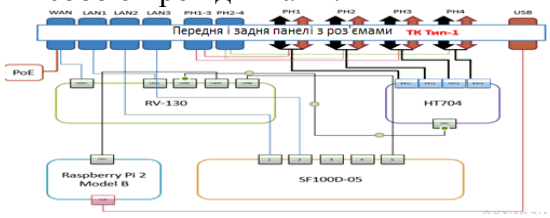


Рис. 1. Схема з’єднання між собою пристроїв

Як і будь-який пристрій ТК-1 має тенденцію „старіти”, оскільки переважна більшість його складових зняті з виробництва і мають більш нові та потужніші аналоги. В дослідженні можливої модернізації як технічної (апаратної) так і програмної пропонується наступне: замінити „устарівший” мікрокомп’ютер на більш потужний Raspberry Pi 3 Model B+; замінити знятий з виробництва маршрутизатор Cisco RV-130 на більш нові аналоги цієї ж компанії, при можливості замінити маршрутизатор та комутатор на один пристрій; провести більш якісну розпайку портів і обладнання задля збільшення місця; додати 5-7 дюймовий дисплей для виводу інформації; встановити та відповідно налаштувати повноцінну операційну систему в поєднанні з програмним комплексом Енігма. **Висновок.** Представлений варіант модернізації та вдосконалення ТК-1 дозволяє: по-перше оновити апаратну частину більш сучасним обладнанням; по-друге зменшити кількість обладнання під корпусом ТК-1 використавши вільне місце під акумулятор більшого об’єму, що в свою чергу покращить автономність; по-третє поєднавши програмний комплекс Енігма з повноцінною операційною системою Raspbian перетворити ТК-1 в повноцінне робоче місце адміністратора.

к.т.н. Бугайов М. В. (ЖВІ)
Калетинець Р. В. (ЖВІ)

МЕТОДИКА ВИЗНАЧЕННЯ ПАРАМЕТРІВ РАДІОПЕРЕДАЧ ЗІ ШВИДКОЮ ПРОГРАМНОЮ ПЕРЕБУДОВОЮ РОБОЧОЇ ЧАСТОТИ ТА ЧАСТОТНОЮ МАНІПУЛЯЦІЄЮ

Актуальність. Для забезпечення завадозахищеності та скритності сучасних засобів радіозв'язку спеціального призначення використовують режим надкороткої пакетної передачі з програмною перебудовою робочої частоти (ППРЧ), що використовує короткочасну передачу інформації в ефір на різних частотах [1 – 2]. Такі цифрові радіостанції працюють, як правило, в режимі швидкої ППРЧ (швидкість перебудови робочої частоти більша за символьну швидкість та перевищує 1000 змін за секунду) і використовують значну кількість частотних каналів (кілька тисяч) з частотним рознесенням між сусідніми каналами, що значно менше ширини спектру частотного елементу. Основним видом модуляції в таких радіостанціях є частотна маніпуляція (ЧМн). Вказані особливості даних радіостанцій зумовлюють необхідність розроблення відповідних методик визначення параметрів сигналів зі швидкою ППРЧ.

Завданням дослідження є розроблення методики визначення параметрів радіосигналів зі швидкою ППРЧ та частотною маніпуляцією в умовах прийому на фоні шумів та в каналі із завмираннями.

Основні положення. Для швидкої ППРЧ розширення спектру досягається за рахунок рознесення символів тривалістю T_s на незалежні частотні елементи (субсимволи), кожен з яких передається почергово на своїй частоті. Часовий інтервал між переключеннями частот (тривалість частотного елемента T_h) характеризує час роботи на одній частоті [1]. При цьому $T_h = T_s/L$, де L − кількість частотних елементів, на які розбивається інформаційний символ. Основним видом інформаційної модуляції при передачі даних в системах зі швидкою ППРЧ є M-на некогерентна ЧМн, причому $M=2^l$, $l \in N$. В межах тривалості частотного елементу T_h сигнал передається на частоті f_{ri}. Крок сітки частот незмінний і складає Δf, а рознесення частот ЧМн − ΔF.

Ідентифікація сигналів зі швидкою ППРЧ і ЧМн здійснюється шляхом оцінювання швидкості перебудови частоти $R_h=1/T_h$, швидкості передавання інформації, кількості частотних каналів N_h і кроку сітки частот Δf та порівняння отриманих значень з відповідними характеристиками відомих радіостанцій зі швидкою ППРЧ.

Оскільки для радіостанцій зі швидкою ППРЧ крок сітки частот Δf, як правило, менший ширини спектру частотного елементу $1/T_h$, тому спочатку необхідно визначити часові межі кожного частотного елементу і в даних межах оцінити його частоту. Для цього розраховують комплексну обвідну сигналу, а точки перетину деякого порогового рівня γ з даною обвідною і визначатимуть межі частотних елементів. Через влив завмирань та адитивного шуму обвідна сигналу буде сильно порізаною тому її згладжують із використанням вікна ковзаючого середнього довжиною P. Значення порогу γ визначають для заданої ймовірності перевищення його шумовим відліком обвідної. Експериментальним шляхом було отримано вираз для розрахунку значення порогу:

$$\gamma = 0{,}216 - 0{,}155\beta P^{-0{,}5},$$

де β − значення квантиля стандартного нормального розподілу.

Для визначення частот частотних елементів f_{ri} використано незгладжені періодограмні оцінки, а підвищення точності визначення частоти при фіксованій довжині вікна аналізу швидкого перетворення Фур'є досягається за рахунок експоненціальної екстраполяції дискретного спектру потужності.

Для визначення кроку сітки частот Δf та рознесення частот ЧМн ΔF необхідно проаналізувати не менше ніж N_h частотних елементів. Якщо ж кількість прийнятих частотних елементів $N_r<N_h$, то однозначно встановити значення Δf і ΔF досить складно.

Шляхом аналізу гістограми різниць $diff(f_{ri})$ відсортованого за зростанням вектора частот частотних елементів визначають крок сітки частот Δf, рознесення частот ΔF та кратність ЧМн M. На рис. 1 наведено гістограму значень параметрів $\Delta f–\Delta F$, Δf *і* $\Delta f+\Delta F$ при $N_r=N_h$ для випадку двійкової ЧМн. У загальному випадку кількість мод у гістограмі складає $2M–1$, а їх очікувані значення становлять $\Delta f \pm m\Delta F$, $m=0..M-1$. Таким чином за формою гістограми можна оцінити кратність ЧМн.

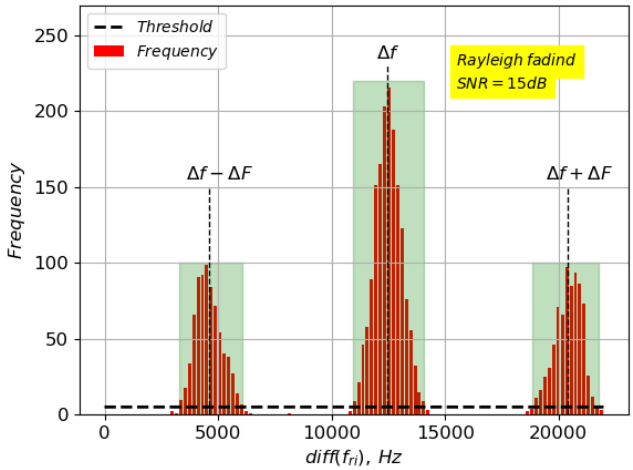


Рис. 1 − Гістограма значень параметрів Δf-ΔF, Δf і Δf+ΔF при $N_r=N_h$

Наближену оцінку кількості частотних каналів N_h обчислюють як відношення розмаху вектора частот частотних елементів $max(f_{ri})– min(f_{ri})$ до кроку сітки частот Δf. Передавання символів при ЧМн здійснюється, як правило, на ортогональних частотах, тому наближено можна вважати, що символьна швидкість складає $R_s=\Delta F$, тобто тривалість символа становить $T_s\approx 1/\Delta F$. Швидкість передавання інформації можна встановити лише після демодуляції сигналу та аналізу бітових потоків, в результаті якого можна визначити структуру кадрів і кількість службових та інформаційних бітів. Кількість службових бітів складає, як правило, близько 20 − 30 % від загальної кількості.

Висновки. Наукова новизна запропонованого методу полягає в розроблених підходах до визначення часових меж частотних елементів на основі порогового оброблення комплексної обвідної та оцінювання кроку сітки частот, рознесення частот та кратності ЧМн на основі аналізу гістограми різниць відсортованого масиву частот частотних елементів. Запропонований метод забезпечує оцінювання значень параметрів сигналів з відносною помилкою, що не перевищує 0,3 %, при значеннях відношення сигнал-шум не нижче 5 дБ. Достовірність отриманих наукових результатів підтверджується результатами математичного моделювання. Отримані результати можуть бути використані при розробленні алгоритмів демодуляції радіосигналів зі швидкою ППРЧ та ЧМн.

Перспективи подальших досліджень пов’язані з розробленням методів ідентифікації та демодуляції радіосигналів зі швидкою ППРЧ та іншими видами смугової модуляції.

ЛІТЕРАТУРА

1. Макаренко С. И., Иванов М. С., Попов С. А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. Монография. СПб.: Свое издательство, 2013. 166 с.

2. Кувшинов О. В., Гурський Т. Г., Гриценок К. М., Шишацький А. В. Аналіз режимів роботи та перспектив бойового застосування сучасних військових УКХ радіостанцій іноземного виробництва // Збірник наукових праць ВІТІ № 1, 2018. С. 43 − 50.

к.т.н. Василенко С.В. (ІСЗЗІ НТУУ „КПІ”)

КОДУВАННЯ СИНХРОМІТКИ ПІДСИСТЕМИ ВХОДЖЕННЯ В СИНХРОНІЗМ СИСТЕМИ РАДІОЗВ’ЯЗКУ З ПСЕВДОВИПАДКОВИМ ПЕРЕНАНЛАШТУВАННЯМ РОБОЧОЇ ЧАСТОТИ

Одним з методів розширення спектру, що використовується у системах радіозв’язку спеціального призначення (СРЗ СП) є метод псевдовипадкового переналаштування робочої частоти (ППРЧ). Головною вимогою, що ставиться до СРЗ з ППРЧ, є необхідність точної часової синхронізації внутрішніх годинників передавача та приймача.

На початковому етапі входження в синхронізм передавач та приймач СРЗ з ППРЧ здійснюють обмін синхрокадрами. Кожен синхрокадр складається з синхромітки, що містить інформацію про номер частотної позиції та номер підциклу в циклі входження та блоку службової інформації, у якому можуть передаватися дані про режим роботи радіостанції, номер абонента, швидкість кодування і.т.д. При прийомі синхрокадру приймач спочатку оцінює синхромітку і за отриманими даними визначає момент часу передачі інформації на частотах входження в синхронізм.

Відомо, що при передачі по каналу радіозв’язку сигнал піддається впливу різного роду завад (у тому числі навмисних), що призводить до втрати певної кількості інформаційних біт синхромітки. На приймальній стороні навіть одна помилка (спотворення одного біту) може призвести до зриву процесу входження в синхронізм. Отже питання забезпечення завадостійкості синхромітки є дуже важливим.

З метою підвищення завадостійкості СРЗ з ППРЧ, дані синхромітки необхідно кодувати. Вибір для кодування оптимальних кодових послідовностей дозволить значно підвищити завадостійкості підсистеми входження в синхронізм СРЗ з ППРЧ.

Відомо, що у широкосмугових СРЗ СП широкого використання набули методи кодування, що засновані на бінарних псевдовипадкових послідовностях Голда, Касамі та М-послідовності. Головною характеристикою даних кодових послідовностей є максимальний сплеск функції взаємної кореляції (R_{max}), що вказує на ступінь кореляції послідовності. Також кодові послідовності характеризуються довжиною послідовності (L), розрядністю регістру зсуву (k) та об’ємом вибірки з послідовності (V).

Аналіз кодових послідовностей показав, що на відміну від інших кодових послідовностей, М-послідовності (послідовності максимальної довжини), які формуються за допомогою регістрів зсуву зі зворотними зв'язками, характеризуються найнижчими значеннями R_{max}. Однак, дані кодові послідовності мають не значні значення V, що вносить додаткову надлишковість, і при великому об’ємі синхромітки призведе до збільшення пропускної здатності радіоканалу.

Використовуючи кодові послідовності Голда, що генерується шляхом сумування по модулю 2 двох М-послідовностей однакової довжини, відбувається збільшення значення V. У цьому випадку отримуємо кодову послідовність такої ж довжини як і М-послідовність, але із значно більшим значенням V. Також, дана кодова послідовність має різні значення R_{max} для парних і непарних значень k.

Кодова послідовність Касамі формується за допомогою трьох послідовних регістрів зсуву з різними зворотними зв’язками, кожен з яких формує свою М-послідовність. Тобто відбувається процес вибірки (децимації) М-послідовності з послідовності Голда з подальшою комбінованою обробкою послідовності Голда вже сформованою послідовністю Касамі. Кодові послідовності Касамі,у порівнянні з М-послідовностями мають більші значення V при не значних значеннях R_{max}. Слід також відмітити, що у порівнянні з М-послідовністю, значення V значно зростає зі збільшенні значення L.

Розглянуті кодові послідовності можуть бути використані для кодування синхромітки підсистеми входження в синхронізм СРЗ з ППРЧ. Вибір конкретної кодової послідовності повинен здійснюватися відповідно до вимог, що ставляться до СРЗ СП.

д.т.н. Василишин В.І. (ХНУПС)
Лютов В.В. (ХНУПС)

ОЦІНЮВАННЯ ПЕРЕДАТОЧНОЇ ХАРАКТЕРИСТИКИ КАНАЛУ ЗВ'ЯЗКУ В OFDM-СИСТЕМАХ З ВИКОРИСТАННЯМ МЕТОДУ SSA

Вимоги щодо покращення характеристик засобів радіозв'язку на сьогоднішній день можуть бути забезпечені шляхом впровадження сучасних методів обробки сигналів та телекомунікаційних технологій. Прикладами таких технологій є OFDM (Orthogonal Frequency-Division Multiplexing – мультиплексування з ортогональним частотним розділенням сигналів), MIMO (multiple input-multiple output – система з багатьма входами та виходами), та їх модифікації. Впровадження сучасних методів обробки сигналів є можливим за рахунок того, що сучасні засоби радіозв'язку є програмно-керованими (SDR –software defined radio).

Покращення ефективності систем радіозв'язку з OFDM, MIMO-OFDM можна досягти за рахунок розподілу потужності сигналу між підканалами OFDM (відключення піднесучих з низьким відношенням сигнал-шум), оцінювання стану каналу зв'язку (передаточної характеристики (функції) каналу зв'язку, якою ідентифікується канал) та використання інформації про стан каналу на передавальній чи приймальній сторонах системи. На приймальній стороні за результатами оцінювання стану каналу зв'язку може здійснюватися корекція амплітуди і фази несучої OFDM-сигналу.

Покращення процедури оцінювання каналу зв'язку та етапів обробки сигналу в приймальній частині OFDM системи можна досягти шляхом використання методів пониження шуму в спостереженні. До сучасних методів пониження шуму в спостереженні відноситься сингулярний спектральний аналіз (SSA-singular spectrum analysis), вейвлет перетворення та інші.

Мета даної роботи, яка полягає в покращенні процедур оцінки каналу зв'язку та обробки сигналу в приймачі OFDM системи, досягається на основі використання методу SSA. В основі методу SSA лежить спектральне розкладення матриці даних або відповідної кореляційної матриці (singular value decomposition (SVD) або eigenvalue decomposition (EVD)).

Прийнятий OFDM символ (після усунення циклічного префіксу CP) надходить до блоку, що реалізує метод SSA (блоку попередньої обробки сигналу). Отриманий на виході сигнал подається як на вхідний перетворювач (S/P), так і на блок оцінювання передаточної характеристики каналу. Попередня оцінка передаточної характеристики може бути отримана з використанням методу найменших квадратів або мінімальної середньоквадратичної похибки. Надалі отримується покращена оцінка з використанням методу SSA. Покращення характеристик традиційного методу SSA може досягатися шляхом врахування особливостей оцінювання дисперсії шуму (використанням модифікованого методу SSA), обчисленням коефіцієнту кореляції Пірсона (зваженого коефіцієнту кореляції) для відбору сигнальних власних векторів на етапі відновлення кореляційної матриці сигналу.

Для оцінки ефективності запропонованого підходу проведене імітаційне моделювання в середовищі MathLab. Результати імітаційного моделювання підтверджують, що використання методу SSA дозволяє зменшення імовірність бітових помилок (BER) та середньоквадратичну похибку оцінювання передаточної характеристики каналу.

До напрямків подальших досліджень слід віднести узагальнення запропонованого підходу на випадок використання в OFDM-системі вейвлет перетворення замість швидкого перетворення Фур'є, методів адаптивної фільтрації в блоці оцінювання передаточної характеристики каналу.

Власенко О.В. (ВІТІ)
Горгуленко В.А. (ВІТІ)
Андрусенко В.В. (ВІТІ)

ЗАСТОСУВАННЯ СИСТЕМ КЕРУВАННЯ БАЗАМИ ДАНИХ *NOSQL* В СТВОРЕННІ ІНФОРМАЦІЙНИХ СИСТЕМ ЗСУ

З початком Операції об'єднаних сил на Сході України явною стала необхідність до модернізації та оновлення інформаційних систем та ресурсів Збройних сил України. На даний час стрімко змінюються вимоги до архітектурної побудови інформаційних систем, на основі чого змін набувають і способи розробки програмного забезпечення. Ці зміни торкаються і, насамперед, веб-додатків, які становлять значну частину новітніх інформаційних ресурсів, в яких, у свою чергу, одним з найважливіших елементів є зберігання та доступ до даних. На сьогоднішній день великого розвитку набули системи керування базами даних (СКБД), засновані на підході *NoSQL*, що отримали популярність завдяки вищим показникам ефективності у порівнянні з класичним реляційним підходом, а саме, швидкодії. *NoSQL* бази даних все більше і більше використовуються в задачах із застосуванням великих даних у веб-додатках реального часу. Мотиви цього підходу включають: простоту дизайну схеми баз даних (БД), значно спрощене горизонтальне масштабування на кластери машин, і тонкий контроль над доступністю. Структури даних, що використовуються в *NoSQL* є відмінними від тих, що використовуються за замовчуванням в реляційних базах даних, що робить тим самим деякі операції над даними значно швидшими на *NoSQL*. Іноді структури даних, які використовуються в *NoSQL* базах даних можуть розглядатись як більш гнучкі ніж таблиці реляційних моделей. В даній роботі розглянуто відмінності застосування реляційного підходу на прикладі СКБД *MySQL* та нереляційного підходу на прикладі СКБД *MongoDB* в розробленій підсистемі адміністрування веб-порталу. Підсистема адміністрування призначена для управління вебпорталом, який містить в собі дані, до яких виконуються запити з високою інтенсивністю. Для проведення експерименту з визначення оптимальної СКБД було розроблено аналогічні БД засобами обидвох з вище вказаних.

Таблиця 1

Порівняння оброки запитів до БД *MySQL* та *MongoDB*

		Кількість пошукових запитів				
		200	400	600	800	1000
Час обробки у СКБД, с	*MySQL*	10	21	29.5	42	51.5
	MongoDB	8.5	16.5	25	33	41

Таблиця 1 демонструє результати експерименту, суттю якого є послідовне надсилання встановленої кількості запитів пошуку до баз даних *MongoDB* та *MySQL* та порівняння часу, витраченого на їх обробку. Результати показують, що для оброки 1000 запитів пошуку реляційній БД необхідно 51.5 секунд, а нереляційній 41 секунду, тобто на 10.5 секунд менше. Проаналізувавши застосування *NoSQL* у веб-середовищі, а саме, як засіб керування даними в підсистемі адміністрування веб-порталу було виділено наступні переваги цього підходу*:*

1. Зберігання великих обсягів неструктурованої інформації. База даних *NoSQL* не накладає обмежень на типи даних, що зберігаються. Більш того, при необхідності в процесі роботи можна додавати нові типи даних.

2. Швидка розробка. Використовуючи *agile*-методи при розробці системи, застосування реляційної БД здатне уповільнити роботу. *NoSQL* бази даних не потребують того ж обсягу підготовчих дій, які зазвичай потрібні для реляційних баз. Отже, використання нереляційних систем керування базами даних значною мірою підвищує ефективність і швидкодію роботи веб-додатків та є доцільним для розробки та модернізації інформаційних систем Збройних сил України.

Власенко О.В. (ВІТІ)
Горгуленко В.А. (ВІТІ)

ЗАСТОСУВАННЯ СИСТЕМ КЕРУВАННЯ БАЗАМИ ДАНИХ *NOSQL* ДЛЯ МОДЕРНІЗАЦІЇ ВІЙСЬКОВИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Ситуація, що склалася на початку антитерористичної операції на Сході України показала необхідність до реформування та оновлення Збройних сил України. У тому числі це стосується інформаційних систем та ресурсів. Необхідною є модернізація наявної складової інформаційного забезпечення Збройних сил України до норм новітніх технологій, що постійно розвиваються, а також створення нового. Вище вказане є невід'ємною частиною успішного ведення інформаційної боротьби та приведення армії у відповідність до стандартів НАТО. Однією з невід'ємних складових розвитку військових інформаційних систем є забезпечення безпечного, стійкого та швидкого доступу до даних. На даний час стрімкого розвитку набули системи керування базами даних, засновані на нереляційному підході зберігання даних. Цей розвиток зумовлений насамперед вивченням реляційного підходу та аналізом його негативних характеристик протягом довгострокового домінування реляційних СКБД.

Отже, постає наступна мета роботи: провести аналіз нереляційного підходу зберігання даних, основних принципів побудови баз даних у системах керування базами даних *NoSQL* та визначити способи застосування *NoSQL* СКБД для модернізації наявних та розробки новітніх інформаційних систем.

NoSQL бази даних все більше і більше використовуються в задачах із застосуванням великих даних *web*-застосунках реального часу. *NoSQL* системи також називають „*Not only SQL*" (англ. *not only SQL* – не тільки *SQL*) для підкреслення того, що вони можуть підтримувати SQL-подібну структуру та мову запитів. Мотиви цього підходу включають: простоту дизайну схеми БД, значно спрощене горизонтальне масштабування на кластери машин (що є проблемою для реляційних баз даних), і тонкий контроль над доступністю. Структури даних, що використовуються в *NoSQL* (такі як ключ-значення, сховище з широким стовпчиком, граф, документ) є відмінними від тих, що використовуються за замовчуванням в реляційних базах, що робить тим самим деякі операції над даними значно швидшими на *NoSQL*. Точна відповідність використання *NoSQL* бази даних залежить від проблем, які треба вирішити. Іноді структури даних, які використовуються в *NoSQL* базах можуть розглядатись як більш гнучкі ніж таблиці реляційних моделей. Підсумовуючи вище вказане було виділено такі переваги баз даних *NoSQL:*

Зберігання великих обсягів неструктурованої інформації. База даних NoSQL не накладає обмежень на типи даних, що зберігаються. Більш того, при необхідності в процесі роботи можна додавати нові типи даних.

Використання хмарних обчислень і сховищ. Хмарні сховища – відмінне рішення, але вони вимагають, щоб дані можна було легко розподілити між кількома серверами для забезпечення масштабування. Використання, для тестування і розробки локального устаткування, а потім перенесення системи в хмару, де вона і працює – це саме те, для чого створені *NoSQL* бази даних.

Швидка розробка. Використовуючи *agile*-методи при розробці системи, застосування реляційної БД здатне уповільнити роботу. *NoSQL* бази даних не потребують того ж обсягу підготовчих дій, які зазвичай потрібні для реляційних баз.

Отже, проаналізувавши нереляційний підхід зберігання даних, принципи побудови баз даних в нереляційних СКБД було продемонстровано ключові переваги *NoSQL*. На основі цього можна зробити висновок, що використання нереляційного підходу зберігання даних (*NoSQL*) є значною мірою доцільним для розробки та модернізації інофрмаційних систем Збройних сил України, а найкращого результату можливо досягти при застосуванні нереляційних баз даних у *web*-середовищі.

к.ф.-м.н. Войтович М.І. (НАСВ)
к.т.н. Ліщинська Х.І. (НАСВ)
к.ф.-м.н. Пак Р.М. (НАСВ)
к.ф.-м.н. Сеник А.П. (НУЛП)

ВПРОВАДЖЕННЯ ДИСТАНЦІЙНИХ ФОРМ НАВЧАННЯ ДЛЯ ВДОСКОНАЛЕННЯ ПІДГОТОВКИ ВІЙСЬКОВИХ ФАХІВЦІВ

Актуальність. Зростаюча швидкими темпами інформатизація всіх сфер діяльності людини вимагає радикальних заходів з організації та модернізації професійної освіти, в тому числі військової. Актуальність питання вдосконалення військової освіти полягає в специфіці 24/7 графіка роботи, оперативності виконання завдань та розміщення пунктів несення служби в різних, часто віддалених, географічних точках.

Постановка задачі. Військова освіта спрямована на навчання слухачів спеціалізованим навичкам, необхідним у майбутньому бою. Принциповими відмінностями між цивільною та військовою освітою є їхні цілі, мотивація та цільове застосування. У традиційній цивільній освіті досягнення вимірюються знаннями, отриманими з лекційної програми, в той час як мета військової освіти полягає в перетворенні курсанта на військового фахівця-практика. Після досягнення початкового рівня знань офіцер може продовжувати освіту, маючи практичний стаж роботи на посаді. Зважаючи на свої службові обов'язки, штатним офіцерам рідко вдається залишити свої місця служби, щоб пройти курси в традиційному військовому навчальному закладі. Тому онлайн-курс є сучасною тенденцією військової підготовки. Системи дистанційного та електронного навчання для військової освіти стали поширеними в останні роки через зростаючу потребу в навчанні офіцерів, викликаною швидкими змінами сценаріїв міжнародних конфліктів.

Мета. Використання технологій дистанційного навчання з застосуванням віртуального навчального середовища для вдосконалення підготовки військових фахівців.

Основні положення. Методи дистанційного навчання можуть значно підвищити рівень підготовки сержантів та офіцерів. Технології дистанційного навчання можуть бути використані для підвищення ефективності стратегій, спрямованих на зменшення дефіциту персоналу, що належить до ключових військових спеціальностей. Дистанційне навчання також може забезпечити стабільність персоналу та зменшити гостроту проблеми забезпечення офіцерським та сержантським складом, виконуючи практичні кроки для завершення необхідної підготовки. Тому необхідно внести відповідні зміни до інвестиційних планів збройних сил з метою підтримки та розвитку програм дистанційного навчання. Наприклад, в країнах членах НАТО постійно збільшуються інвестиції, спрямовані на розвиток інфраструктури дистанційної форми освіти. Це стосується практичних розробок навчальних програм для перекваліфікації військовослужбовців діючих підрозділів від надлишкових до дефіцитних військових професій. Збройні сили також повинні використовувати найбільш гнучкі методи дистанційного навчання для підтримки цієї мети, наприклад, розвиток асинхронного навчального програмного забезпечення на курсах для офіцерів та інших військовослужбовців.

Пріоритетною є технологія дистанційного навчання з використанням віртуального навчального середовища (ВНС) (virtual learning environment) − програмної системи, що створена для підтримки процесу дистанційного навчання. Вдалою системою є діяльність навчального середовища Moodle в Національному університеті „Львівська політехніка", а також впровадження представленої платформи для розвитку дистанційної освіти в Національній академії сухопутних військ імені гетьмана Петра Сагайдачного.

Висновки. Практична реалізація віртуального навчального середовища дозволяє істотно підвищити якість освітнього процесу в спеціалізованих навчальних закладах і забезпечує досягнення його кінцевої мети – підготовку військових фахівців, рівень яких відповідає сучасним вимогам, здатних успішно виконувати завдання, що стоять перед ними.

Голуб’ятніков А.С. (НУБіП України)
к.п.н. Блозва А.І. (НУБіП України)

БРАНДМАУЕРИ – ОСНОВА МЕРЕЖЕВОЇ БЕЗПЕКИ

Актуальність дослідження пов’язана з необхідністю впровадження міжмережевих екранів та набору правил на маршрутизаторах, які встановлюють політику щодо трафіка який циркулює по мережі.

Мета. Здійснити аналіз основних програмних та апаратних засобів, які реалізують політику управління доступом по мережі.

Виклад основного матеріалу

Організації повинні використовувати захист в глибину для виявлення загроз і захисту вразливих ресурсів. При такому підході використовуються кілька рівнів безпеки на периметрі мережі, в самій мережі і на кінцевих мережевих пристроях.

Наприклад, на рис.1 показана проста топологія захисту в глибину.

Рис. 1. Проста топологія захисту в глибину

Першою лінією захисту є граничний машрутизатор (R1). Він містить набір правил, що вказують, який трафік має дозволятись, а який – заборонятись, а також передає всі підключення, призначені для внутрішньої локальної мережі, на міжмережевий екран.

Другий лінією захисту є міжмережевий екран (Firewall). Це контролюючий пристрій, який виконує додаткову фільтрацію і відстежує стан підключень. Він забороняє ініціювання підключень від зовнішніх (ненадійних) мереж до внутрішньої (надійної) мережі і дозволяє внутрішнім користувачам встановлювати двосторонні підключення до ненадійних мереж

Внутрішній маршрутизатор представляє собою ще одну лінію захисту (R2). Може виконувати остаточну фільтрацію трафіка перед його пересиланням до місця призначення.

Маршрутизатор і брандмауер – це не єдині пристрої, які використовуються в захисті в глибину. Іншими такими пристроями є системи запобігання вторгнень (IPS), захист від складного шкідливого ПО (AMP), системи забезпечення безпеки веб-вмісту та електронної пошти, служби ідентифікації, засоби контролю доступу до мережі та інші[1].

Брандмауер – це система або група систем, що реалізує політику управління доступом між мережами.

Переваги:

стійкі до мережевих атак;

представляють собою єдину транзитну точку між внутрішніми корпоративними мережами і зовнішніми мережами, так як весь трафік проходить через міжмережевий екран;

застосовують політики управління доступом;

запобігають доступу неавторизованих користувачів до конфіденційних хостам, ресурсів і додатків.

блокування шкідливих даних від серверів і клієнтів;

зниження складності управління безпекою за рахунок розподілу більшості функцій контролю доступу до мережі з кількох міжмережевих екранів, які є в мережі.

Але брандмауери також мають і деякі обмеження:

неправильно налаштований міжмережевий екран може привести до серйозних наслідків для мережі, наприклад, стати єдиною точкою відмови;

дані з багатьох додатків, не вдасться надіслати через міжмережеві екрани надійним чином;

користувачі можуть за власною ініціативою шукати шляхи обходу брандмауера для отримання заблокованого матеріалу, що піддає мережу ризику потенційних атак;

може знижуватися продуктивність мережі;

неавторизований трафік може тунелюватись або маскуватися під трафік, якому дозволено проходити через міжмережевий екран[2].

Головне в брандмауері – це визначення інтерфейсів пристроїв, які дозволяють або забороняють трафік в залежності від джерела, місця призначення та типу трафіка. Найпростіший варіант – призначення зовнішньої мережі і внутрішньої мережі, які визначаються двома інтерфейсами на межмережевому екрані. Як показано на рис. 2, загальнодоступна (або зовнішня) мережа є недовіреною, а приватна (або внутрішня) мережа є довіреною. Як правило, міжмережевий екран з двома інтерфейсами налаштовується наступним чином.

1) Трафік, що виходить із приватної мережі, дозволяється і перевіряється при передачі його в загальнодоступну мережу. Перевірений трафік, що повертається із загальнодоступної мережі і пов'язаний з трафіком, що походить із приватної мережі, дозволяється.

2) Трафік, що виходить із загальнодоступної мережі і надходить у приватну мережу, зазвичай блокується.

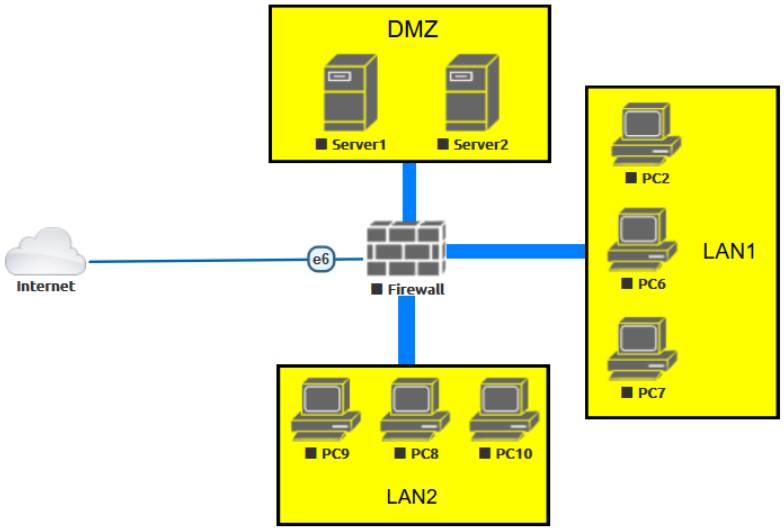


Рис. 2. Міжмережевий екран на основі зональної політики

Висновки.

Міжмережеві екрани на основі зональних політик використовують концепцію зон, яка забезпечує додаткову гнучкість. Зона – це група, що складається з одного або декількох інтерфейсів з подібними функціями і призначенням. Зони дозволяють вказувати, де повинна застосовуватися політика або правило брандмауера. За замовчуванням до трафіка між інтерфейсами в одній зоні ніяка політика не застосовується, і він проходить вільно. Однак, весь трафік між зонами блокується. Для того, щоб трафік міг проходити між зонами, необхідно налаштувати політику для дозволу або перевірки трафіка.

ЛІТЕРАТУРА

1. Cisco Networking Academy [Електронний ресурс]: Определение угроз – Режим доступу: https://static-course-assets.s3.amazonaws.com/CyberOps11/ru/index.html#8.1.1.4

2. Cisco Networking Academy [Електронний ресурс]: Межсетевые экраны– Режим доступу: https://static-course-assets.s3.amazonaws.com/CyberOps11/ru/index.html#5.2.1.2

3. Cisco Networking Academy [Електронний ресурс]: Распространенные архитектуры безопасности – Режим доступу: https://static-course-assets.s3.amazonaws.com/CyberOps11/ru/index.html#5.3.1.7

к.т.н. Горбенко В.І. (ВІТІ)
Мартошенко М.В. (ВІТІ)

НАВЧАЛЬНО ІНФОРМАЦІЙНА ПІДСИСТЕМА З ДИСЦИПЛІНИ „СИСТЕМНЕ ПРОГРАМУВАННЯ ТА АРХІТЕКТУРА КОМП'ЮТЕРА"

Створення та функціонування інформаційних систем в процесах управління підрозділами (частинами) Збройних сил України тісно пов'язане з розвитком інформаційних технологій – головною складовою сучасних автоматизованих інформаційних систем спеціального призначення.

Сучасна інформаційна технологія орієнтована на застосування найширшого спектру технічних засобів електронно-обчислювальних машин і засобів комунікацій. На її основі створено та створюються обчислювальні системи й мережі різних конфігурацій не тільки для нагромадження, зберігання, перероблення інформації, але й максимального зближення термінальних улаштувань до робочого місця спеціаліста та для підтримки прийняття відповідних рішень на управління.

Основу нової інформаційної технології складають розподілена обчислювальна техніка, „дружнє" програмне забезпечення та сучасні засоби комунікації. Принципова відміна нової інформаційної технології полягає не тільки в автоматизації процесів зміни форми й розміщення інформації, а й у зміні її змісту.

Інформаційна система виконує функції збирання, зберігання, розповсюдження і обробки інформації.

На рис.1 наведені функції інформаційної системи через її основні структурні компоненти.

Рис. 1 Визначення інформаційної системи

Навчально-інформаційна система − це сховище інформації, яке включає засоби введення, зберігання, захисту, пошуку і подання повідомлень.

Навчальна інформаційна система є складовою інформаційних систем закладів освіти і призначена для надання доступу користувачам до навчальних інформаційних ресурсів, а також контролю знань студентів і аспірантів. Складовими навчально інформаційних систем є навчальні інформаційні ресурси, інструментарій користувачів, інтерфейси користувачів, підсистема контролю успішності.

Навчально інформаційна підсистема з дисципліни „системне програмування та архітектура комп'ютера" призначена для використання у навчальному процесі з підготовки спеціалістів з інформаційних технологій.всі висунуті вимоги до подібних систем і забезпечує підвищення якості підготовки курсантів за рахунок автоматизації процесу вивчення навчальної дисципліни „СПАК".

к.т.н. Горбенко В.І. (ВІТІ)
Сачок О.М. (ВІТІ)

ПІДСИСТЕМА ОБЛІКУ ЗАСОБІВ ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ НАВЧАЛЬНО-ЛАБОРАТОРНОГО КОМПЛЕКСУ КАФЕДРИ ВВНЗ

Процес обліку військового майна у Збройних силах України ведеться згідно наказу МОУ № 440 від 17.08.2017 „Про затвердження Інструкції з обліку військового майна у ЗСУ" додаток 13 з метою отримання даних про його наявність, втрату, нестачу, рух, вартість та якісний (технічний) стан, необхідних для організації матеріально-технічного забезпечення військових частин, встановлення належного контролю за умовами зберігання, законністю, доцільністю та ефективністю використання (витрачання), а також з метою підготовки даних для складання облікових і звітних документів та державної статистичної звітності [1]. Сучасний стан ведення обліку майна вимагає запровадження технічних засобів автоматизації.

У зв'язку зі збільшенням обсягу матеріальних засобів, що знаходяться на обліку в підрозділах та розвитком персональних електронно-обчислювальних машин виникає потреба автоматизувати процес обліку майна для забезпечення підвищення продуктивності праці фахівців у вищих військових навчальних закладах (ВВНЗ) а також у ЗСУ.

Таким чином, розробка підсистеми обліку засобів обчислювальної техніки навчально-лабораторного комплексу кафедри ВВНЗ є актуальною.

У доповіді подаються принципи побудови, структура, алгоритм функціонування підсистеми з метою автоматизації обліку засобів обчислювальної техніки навчально-лабораторного комплексу (НЛК) кафедри ВВНЗ. Пропонується концепція баз даних (БД) замість використовуваної на теперішній час електронної таблиці.

Користувач підсистеми з числа працівників НЛК керує основними таблицями БД, вводить параметри запитів до БД, здійснює фільтрування інформації, пошук і облік майна навчально-лабораторного комплексу кафедри ВВНЗ.

Вихідними даними для створення підсистеми є: кількість, основні характеристики і розташування майна, яке знаходиться на кафедрі ВВНЗ, а також форми обліку та звіту стосовно засобів обчислювальної техніки.

Для розробки підсистеми обліку засобів обчислювальної техніки навчально-лабораторного комплексу кафедри ВВНЗ було обрано мову програмування C# та СКБД MS SQL Server 2017 що дозволяє побудувати підсистему на основі технології клієнт-сервер [2]. Архітектура клієнт-сервер є одним із архітектурних шаблонів програмного забезпечення та є домінуючою концепцією у створенні розподілених мережних застосувань і передбачає взаємодію та обмін даними між ними.

Отже, в доповіді: проаналізовано основні документи, якими регламентується робота щодо обліку майна у ЗСУ; подано принципи побудови, структуру та алгоритм підсистеми обліку засобів обчислювальної техніки НЛК кафедри ВВНЗ.

ЛІТЕРАТУРА

1. Облік військового майна у Збройних силах України: [посіб. для фахівців бюдж. військ, частин, установ та орг. Збройних сил України] / [О.І. Ворона, Р.Т. Джога, В.В. Ткаченко, Г.О. Іва- нов, В.Л. Рихтюк]. – К.: Знання України, 2017. – 512 с.

Information technology - Database languages - SQL – Part 2: Foundation (SQL/Foundation)

к.т.н. Горбенко І.В. (ВІТІ)
Харламов Є.М. (ВІТІ)

ПІДСИСТЕМА МОНІТОРИГНУ ІНФОРМАЦІНОЇ СИСТЕМИ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ З ВИКОРИСТАННЯМ ВЕБ-ТЕХНОЛОГІЙ

Важливість моніторингу інформаційної системи робочих станцій обчислювальної мережі для підтримання їх постійної готовності полягає в безперервному контролі за роботою мережі, що становить основу будь-якої інформаційно-телекомунікаційної мережі, необхідний для підтримки її в працездатному стані. Зважаючи на важливість цієї функції її часто відокремлюють від інших функцій систем управління і реалізують спеціальними засобами. Такий поділ функцій контролю і власне управління корисний для невеликих і середніх мереж і використовується, наприклад, у системі моніторингу *Zabbix* .

Система моніторингу *Zabbix* вже широко використовується у інформаційних технологіях на об’єктах військового призначення. Складається з декількох підсистем, які можуть бути розташовані на різних машинах: сервер моніторингу, база даних (наприклад, *SQLite*, *MySQL*, *PostgreSQL* та *Oracle*), веб-інтерфейс на *PHP*, агент *Zabbix*, *Zabbix proxy*. Підтримує кілька типів моніторингу. *Simple checks* використовується для *SMTP* або *HTTP* без установки додаткового програмного забезпечення. *Zabbix agent* використовується для операційних систем, щоб моніторити стан процесора, використану мережу, дисковий простір. *External check* виконує зовнішні програми. За допомогою даного програмного забезпечення можна відстежувати стан сервісів мережі, серверів та мережевого обладнання. Також є можливість розподіляти навантаження по декількох проксі-сервер, які ділять чергу опитувань об'єктів моніторингу між собою, тим самим вивільняючи додатки до основного сервера. Використання оповіщень та автоматичних дій на основі заготовлених сценаріїв при досягненні порогових значень спостережуваних метрик, можливість прогнозувати подальшу поведінку метрик на основі вже отриманих значень.

Переваги *Zabbix*: конфігурації розміщені в базі, управління відбуваються через інтерфейс; є єдина точка доступу для користувачів; хвилинний інтервал – одиниця між вимірами; з серверів збираються кількісні характеристики роботи, які були проаналізовані на стороні сервера; час зберігання даних обмежено тільки місцем на диску; безліч варіантів аналізу даних, які були зібрані. Недоліки: немає відмовостійкості, дані історії зберігаються в базі, обмежена функціональність для роботи з візуалізацією даних і велика затримка покази значної кількості графіків на одному екрані.

Тому необхідно здійснити розробку підсистеми моніторингу інформаційної системи спеціального призначення на основі розподіленої системи моніторингу *Zabbix,* а саме максимально адаптувати веб-інтерфейс з відокремленим функціоналом основної системи для військових користувачів з будь-яким рівнем знань.

Отже, пропонується розробити підсистему моніторингу інформаційної системи на основі візуалізації результатів моніторингу з використанням системи *Zabbix* для більш адаптивного інтерфейсу і виокремлення функцій його застосування. Так, підсистема дозволить значно підвищити рівень користувачів на об’єктах військового призначення та запобігти виникнення проблем використання в особового складу

ЛІТЕРАТУРА

1. Душин В.К. Теоретичні основи інформаційних процесів та систем: учебник для студ. вузов / В.К. Душин. 4- е изд. М.: Дашков и К., 2010. – 348 с.

2. Waldbusser S. Remote Network Monitoring Management Information Base / S. Waldbusser // RFC 1757. – 1995. – Feb.

к. філос. н. Горлинський В.В. (ІСЗЗІ НТУУ „КПІ”)
д. філос. н. Ананьїн В.О. (ВІТІ)

ВДОСКОНАЛЕННЯ ПІДГОТОВКИ ВІЙСЬКОВИХ ФАХІВЦІВ: БЕЗПЕКОВИЙ АСПЕКТ

Зростання військових, гуманітарних, техногенних і екологічних небезпек, підвищення соціальних ризиків, на думку дослідників, є проявом сучасних світових тенденцій, які вимагають впровадження у підготовку сучасних фахівців теоретичних знань про безпеку, відповідних вмінь, формування безпекових компетентностей. Для військових фахівців сектору безпеки і оборони України дана вимога є особо актуальною, враховуючи військові події на сході країни.

Дослідженню освіти, як чиннику сталого і безпечного розвитку суспільства, присвячені праці В. Андрущенка, В. Галєєва, В. Журавського, М. Згуровського, А. Єрмоленка, М. Кисельова, В. Кулиниченка, В. Лук’янця, М. Нещадима, Б. Новікова, В. Огнев’юка, В. Остроухова, О. Пучкова, В. Смолянюка, В. Ягупова та ін. Але, питання впровадження безпекових знань і компетентностей в систему підготовки фахівців сектору безпеки і оборони України, нажаль, остається досить не достатньо розкритим.

Аналіз змісту наукових праць дозволяє окреслити коло сучасних освітніх пріоритетів, що мають сприяти розв’язанню поставленої проблеми. По-перше, це спрямованість підготовки на формування ціннісних орієнтацій та соціально-психологічних настанов, що зумовлюють відповідальне ставлення до розв’язання питань безпеки в службовій, професійній та соціальній діяльності. По-друге, це переорієнтація спрямованості соціальних, правових і спеціальних освітніх дисциплін на формування безпекових компетентностей. До них можна віднести такі здатності, як морально-психологічна готовність до виконання службового і професійного обов’язку в умовах проведення операції Об’єднаних сил; морально-психологічна стійкість в умовах деструктивного інформаційно-психологічного впливу супротивника; інтелектуальна, моральна, психологічна, правова і службово-професійна здатність до діяльності в умовах зростаючого ризику, воєнних, техногенних і гуманітарних загроз; відповідальність за наслідки власної службової та професійної діяльності; прогнозування, попередження і подолання імовірних небезпек у професійній діяльності; систематичне оновлення знань про можливі небезпеки, загрози і ризики у професійної та повсякденній життєдіяльності; критичне переосмислення і перебудова власної ієрархії ціннісних орієнтацій та психологічних настанов як основи відповідального і безпечного способу життя.

Безумовно, формування окреслених здатностей має здійснюватися системно, протягом професійного навчання всіма кафедрами освітнього закладу, але цілеспрямовано, це має бути забезпечено навчальними дисциплінами з проблем сталого розвитку, морально-психологічного забезпечення професійної діяльності, психології та правознавства, що мають озброювати курсантів системою безпекових знань і компетентностей. Актуальним завданням даних дисциплін є формування інтелектуальної, моральної, психологічної, правової і професійної здатності та готовності людини до діяльності в умовах зростаючого ризику, воєнних загроз, техногенних і гуманітарних небезпек, їх прогнозування, попередження і подолання та формування системи відповідних безпекових компетентностей. Велике значення у формуванні свідомості, світоглядної основи, життєвої позиції майбутнього фахівця сектору безпеки і оборони мають філософські дисципліни, що формують наукове світобачення, переконання, патріотичні громадянські позиції, так необхідні у складний сучасний час.

Висновок. В цілому, проведений аналіз дозволяє зробити висновок про необхідність розробки і впровадження системи гуманітарних безпекових знань, вмінь, навичок і компетентностей в інтересах сталого і безпечного розвитку суспільства як важливої компоненти системи підготовки фахівців сектору безпеки і оборони України.

Грачов О.В. (ТОВ „Радіо Сатком Груп”)

L3HARRIS -РЕЗУЛЬТАТИ ТА НОВІ ПЕРСПЕКТИВИ

Актуальність. Враховуючи постійну та достатньо суттєву допомогу Уряду Сполучених Штатів Америки Україні за контрактами міжнародної військово-технічної допомоги в частині, що стосується надання обладнання зв’язку та аксесуарів компанії Harris Corporation.

Створення в оборонній сфері США компаній L3Harris, шляхом об’єднання двох великих американських компаній Harris Corporation та L3 Technology, яке є одним з найбільших в історії США та є важливою новиною, також і для України.

Мета. Представити результати об’єднання компаній, її напрямки роботи та перспективи які можуть покращити якість військового зв’язку в Україні

Основні положення.

L3Harris – новий оборонні промисловий гігант США, основні показники ринкової вартості, прибуток за 2018 рік та напрямки діяльності компаній (космічні та розвідувальні системи, електронні системи, системи зв’язку):

Системи зв’язку.

Рішення для тактичного та авіаційного зв'язку, пристрої для нічного бачення, мережеві технології для армії та інших силових структур.

Космічні та розвідувальні системи.

Наземні системи прийому та обробки інформації, продукція та аналітика для глобальної та космічної обізнаності та задач огляду Землі.

Електронні системи.

Засоби радіоелектронної боротьби, авіоніка, роботи, рішення C4ISR для армії та інших силових структур та системи гарантованого авіаційного зв'язку для цивільних та військових.

Стратегія розвитку систем зв’язку компанії L3Harris взаємопов’язано з розробкою нових форм сигналів, нових версій програмного забезпечення, нових радіостанцій та модифікації і покращенні існуючих рішень, а саме:

Falcon net ecosystemtm – це система, що складається з усіх елементів необхідних для прийняти рішень та управління боєм в сучасних умовах (обладнання, програмне забезпечення, тактичні застосунки, послуги) поєднаних в одну платформу;

взаємно пов’язані форми сигналів для різних структурних підрозділів військ від рівня бригади до рівня взводу;

Новий, вдосконалений режим – TNW-75 (Time Division Multiple Access (TDMA) Networking Waveform), що дозволяє ефективно використовувати як частотний ресурс так і ресурс обладнання.

В поєднанні з сімейством радіостанцій RF-7850 є майже ідеальним рішенням для сухопутних військ забезпечуючи завадостійкість, передачу тактичної інформації та відсутність критичних вузлів (автоматичне формування та відновлення мережі);

Нова модифікація, що дозволяє суміщати дві портативні радіостанції в одному автомобільному корпусі, який має мінімальні вимоги до розміщення та не потребує додаткових амортизаційних платформ.

Крім вищезазначеного, компанія вдосконалює існуючі програмні платформи під УКХ обладнання (оновлено до версії 4.8.0) та інтерфейс користувача (WEBUI), а також займається впровадженням бездротових інтерфейсів в радіостанції для підключення периферійних пристроїв та датчиків.

Компанією L3Harris, на даний момент вже поставлено більше 100 тис. новітніх КХ радіостанцій (сімейство Falcon III) по всьому світу.

КХ рішення є майже у всіх варіантах виконання – переносний, автомобільний, стаціонарний, авіаційний та морський.

Основним рішенням стратегічного напрямку є КХ система потужністю 1 кВт з рознесеним сторін прийому та передачі, що використовується для зв'язку між штабами, або віддаленими підрозділами (об'єктами) (флот, міжнародні місії та інше).

На сьогодні існує нова версія внутрішнього програмного забезпечення КХ радіостанції – FW 2.1.0, яка має ряд фундаментальних змін, а саме:

Покращена ефективність на поганих каналах.

Максимум 124 РС в 3G замість 50.

SNMP v3.

Новий дизайн меню передньої панелі.

Перегляд SMS та APR у всіх режимах.

Частотний план міняється автоматично по часу.

Зберігання багатьох планів місій.

Оптимізовано управління ключами Citadel/AES.

Полегшене оновлення FW.

Враховуючи суттєвий досвід в розробці авіаційних рішень компанії L3 Technology, компанія L3Harris посилює розвиток вектору розробки та підтримки авіаційних систем для літаків, вертольотів конвертопланів, БПЛА), модельний ряд обладнання для авіації включає в себе як інтегровані рішення так і рішення швидкого встановлення.

Відповідаючи потребам сьогодення, щодо якісного та захищеного зв'язку для БПЛА компанія L3Harris презентувала нову модульну радіостанцію RF-7850A-ER з безпрецедентною вагою та розмірами у поєднанні з широким функціоналом УКХ радіостанції:

Підтримує форми сигналів S-TNW, TNW-25.

Підтримка M-TNW, TNW-75 та ANW2®C запланована в майбутньому.

Окремим і не менш важливим напрямками роботи компанії є виробництва засобів для організації IP мереж, що представлені модельним рядом радіорелейних станцій та багатодіапазонної радіостанції, а також мобільних захищених шлюзів C4I (Command, Communications, Control, Computers and Intelligence).

Розробка та підтримка програмного забезпечення, які призначені для планування радіомереж, зон покриття КХ/УКХ/ДМХ з підтримкою радіостанцій та форм сигналів L3Harris, окремо програмного забезпечення для моніторингу стану мереж з віддаленим контролем та усуненням несправностей а також системи управління боєм.

Висновки.

Об'єднання компаній Harris Corporation та L3 Technology дозволяє збільшити можливості у дослідженнях та розробках нових електронних систем та рішень крім того, нова компанія забезпечує підтримку раніше випущеного обладнання - впровадженням нового функціонала за рахунок Software-defined radio (SDR) технологій.

Використання продукції компанії L3Harris дозволить за рахунок згаданих вище технічних рішень значно підвищити ефективність існуючих комунікаційних та інформаційних систем силових структур та спеціальних відомств України.

к. т. н. Гребенюк О. П. (ЖВІ)
к. т. н. Мартинчук О.О. (ХНУРЕ)
к. т. н. Роговець М. А. (ЖВІ)
Гребенюк О. О.(ЖВІ)

ЗАСТОСУВАННЯ ПОЛЯРИЗАЦІЙНО-ПРОСТОРОВОЇ ОБРОБКИ СИГНАЛІВ ДЖЕРЕЛ РАДІОВИПРОМІНЮВАННЯ ПРИ ДІЇ ЗАВАД В ЗАСОБАХ РАДІОМОНІТОРИНГУ З АНТЕНАМИ ПОДВІЙНОЇ ПОЛЯРИЗАЦІЇ

Воєнно-політична обстановка довкола України залишається напруженою та характеризується довготривалою агресією з боку Російської Федерації проти нашої держави. При цьому, не виключається застосування збройних сил при проведенні широкомасштабних бойових дій у формі повітряно-космічної-наземної наступальної операції. Аналіз досвіду останніх локальних війн та Операції об'єднаних сил свідчить про те, що на початковому етапі проведення наступальних дій здійснюється масоване застосування наземних та повітряних засобів та комплексів радіоелектронної боротьби (радіоелектронної війни) з метою радіоелектронного подавлення систем управління та зв'язку, засобів радіотехнічного забезпечення підрозділів, частин та з'єднань сухопутних військ, військово-повітряних сил та військово-морських сил.

В таких умовах ефективність виявлення та пелентування (місцевизначення) джерел радіовипромінювання (ДРВп) засобами та комплексами радіомоніторингу, насамперед на тактичну глибину в УКХ діапазоні, суттєво погіршиться, що в свою чергу ускладнить (унеможливить) виконання завдань радіомоніторингу у заданих районах.

У зв'язку з цим, актуальним завданням є розробка та застосування в існуючих та перспективних засобах і комплексах радіомоніторингу алгоритмів та пристроїв обробки сигналів на фоні активних завад.

Дослідження такого підходу здійснюється з метою покращення оперативно-технічних показників засобів радіомоніторингу щодо виявлення сигналів ДРВп при дії активних завад.

В основі запропонованого лежить спільне використання в обробці поляризаційних та просторових параметрів (відмінностей) сигналів та завад, які проявляються при застосуванні методу повного поляризаційного приймання.

Технічними передумовами є застосування в якості антени антенної решітки із широкосмуговими по частоті та ортогональними по поляризації антенними елементами, такими як планарні антени, рупори із широкосмуговими вставками, ТЕМ рупори. Наявність ортогональних антенних елементів дозволяє представляти сигнали у вигляді поляризаційних векторів (ПВ) в ході обробки. При цьому необхідно враховувати вплив поляризаційних характеристик антенної системи на параметри ПВ, що є актуальним, оскільки сигнали ДРВп та завад надходять до антенної системи з різних кутових напрямків.

Загалом, використання при обробці в засобах радіомоніторингу поляризаційних та просторових параметрів потенційно створює передумови щодо покращення:

- виявлення сигналів ДРВп в умовах дії активних завад (за умови наявності відмінностей у просторових або поляризаційних параметрах їх сигналів);
- результатів оцінювання кутових координат ДРВп (методи надрозрізнення ДРВп, використання при пелентуванні ДРВп поляризаційних параметрів їх сигналів);
- розпізнавання ДРВп за видами і типами при врахуванні додаткових ознак за поляризаційними параметрами їх сигналів (є актуальним насамперед для радіотехнічного контролю багатофункціональних РЛС, що використовують різні види складних сигналів та режими випромінення).

Для досягнення визначеної мети запропоновано застосування в існуючих та перспективних засобах та комплексах радіомоніторингу повного поляризаційного приймання з оптимізацією поляризаційного базису антенної системи, а також алгоритму просторово-поляризаційної обробки сигналів ДРВп при дії активних завад.

к.т.н. Гуржій П.М. (НЦЗІ ВІТІ)
к.т.н. Коваленко І.Г. (НЦЗІ ВІТІ)
Гуржій І.А. (НЦЗІ ВІТІ)

АНАЛІЗ ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ СПЕЦІАЛІЗОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВЕДЕННЯ РЕЄСТРІВ РАДІОЕЛЕКТРОННИХ ЗАСОБІВ ТА ВИЗНАЧЕННЯ ЇХ ЕЛЕКТРОМАГНІТНОЇ СУМІСНОСТІ

Керівними документами Збройних сил України передбачено створення інформаційної системи, до якої повинні підключатися дані Реєстру радіоелектронних засобів та випромінюючих пристроїв (ВП), що можуть застосовуватися на території України спеціальними користувачами радіочастотного ресурсу України, Реєстру присвоєнь радіочастот для РЕЗ і ВП спеціальних користувачів радіочастотного ресурсу України, а також засоби автоматизованої обробки інформації та пакет інформаційно-розрахункових задач управління РЧР, що дозволить радіочастотним органам ефективно виконувати свої функції. Але на дійсний час в ЗСУ відсутня зазначена інформаційна система та відповідне програмне забезпечення, таким чином існує потреба в розробці або закупівлі спеціалізованого програмного забезпечення для планування мереж зв’язку та розрахунку електромагнітної сумісності радіо засобів.

Основні характеристики та можливості спеціалізованого програмного забезпечення , призначене для зазначених цілей, наведено у таблиці 1

Таблиця 1

Назва ПЗ	**Узагальнені характеристики**
RF3D WiFi Planner	Дозволяє розраховувати невеликі WiFi-мережі. Може використовуватися невеликими операторами бездротового зв'язку або організаціями, які планують власну мережу WiFi.
Ekahau Site Survey	Дозволяє розраховувати невеликі WiFi-мережі. Рекомендується невеликими операторами бездротового зв'язку або організаціями, які планують власну мережу WiFi. Має більш зручний інтерфейс ніж RF3D WiFi Planner.
RVA «Розрахунок впливу антен»	Призначена для проведення розрахунків електромагнітного поля, санітарно-захисних зон і зон обмеження забудови, формування звітів. Корисна при використанні операторам зв'язку, інститутам, радіовипромінюючим центрам.
Atoll	Дозволяє повністю спланувати бездротову мережу зв’язку, та необхідна розробнику мережі на всіх етапах життєвого циклу бездротової мережі, починаючи від дизайну і закінчуючи мережевою оптимізацією. Рекомендується для роботи з великими бездротовими мережами.
ICS Telecom	Вирішує дуже широке коло завдань, починаючи від аналізу існуючих бездротових мереж і закінчуючи їх плануванням. Рекомендується до використання великими операторами зв'язку для планування міських і великих за розміром мереж, недоцільно використовувати при плануванні невеликих за розміром мереж. Рекомендується при плануванні великих бездротових мережам.

Враховуючи досить обмежені можливості та вузькопрофільність програмного забезпечення: RF3D WiFi Planner, Ekahau Site Survey та RVA „Розрахунок впливу антен” більш детально розглянемо СПЗ Atoll та ICS Telecom.

Програмне забезпечення – Atoll виробництва компанії Forsk (http://www.forsk.com/). Призначене для планування бездротової мережі починаючи від дизайну, закінчуючи мережевою оптимізацією. Програмою підтримуються наступні технології: GSM / GPRS / EDGE; UMTS / HSPA; CDMA2000 1xRTT / EV-DO; LTE; TD-SCDMA; WiMAX / BWA; радіорелейні лінії.

Atoll надає деякі функції геоінформаційних систем, а саме: інтегрований картографічний редактор; інтерфейс для взаємодії з іншими геоінформаційними системами: MapInfo, ArcView, Google Earth; підтримку високо якісних карт, та сканованих карт; підтримку векторних і точкових 3D-моделей будівель; підтримку даних про трафік, клімат та населення (для симулювання навантаження на мережу).

Можливості програмного забезпечення Atoll: автоматичне планування і оптимізацію мережі по заданому частотному плану і за бажаним покриттям; автоматизацію дій за допомогою застосування скриптів; вибір різних моделей поширення; можливість виконувати обчислення розподілених в кілька потоків одночасно; створення звітів.

Програмне забезпечення – Atoll це професійний програмний інструмент який потребує професійного підходу в при його використанні. Програма рекомендується для використання для роботи з великими мережами. Інформація про вартість даного програмного забезпечення відсутня у вільному доступі.

Програмне забезпечення – ICS Telecom виробництва компанії ATDI (http://www.atdi.us.com/ICSTelecom.aspx).

Можливості програмного забезпечення: аналіз практично всіх видів бездротових мереж, включаючи мобільні GSM / CDMA / LTE, WiFi / WiMAX, радіорелейні, широкомовні, телеметричні, а також радари, супутникові наземні станції та інше; планування і випробування мереж, рішення задач системного адміністрування, бізнес-моделювання, визначення розмірів інфраструктури і т. д.

Програма працює з проектами, в які входять різні шари: цифрова модель місцевості; зображення карти; колірна палітра; шар перешкод; шар будівель; шар об'єктів зв'язку. ICS Telecom дозволяє проводити аналіз взаємного впливу базових станцій за двома методами, що дозволяє домогтися мінімальної інтерференції, а також скласти економний частотний план.

Програмне забезпечення ICS Telecom побудовано на використанні рекомендації ITU.

ПЗ ICS Telecom дозволяє вести базу даних обладнання, генерувати абонентів, в тому числі і випадковим чином, проводити статистичний аналіз, розраховувати покриття, підбирати автоматично мінімально необхідну висоту для стійкої роботи прольоту радіорелейної лінії та інші параметри потрібні при якісному та детальному плануванні бездротових мереж зв’язку.

Враховуючі можливості програмного забезпечення – ICS Telecom, ціна даного програмного комплексу досить висока та її необхідно уточнювати у виробника або регіонального дистриб'ютора.

Для забезпечення виконання задач з визначення електромагнітної сумісності радіоелектронних засобів (РЕЗ) (в тому числі проведення науково-технічних експертиз радіочастотних заявок) в НЦЗІ ВІТІ було розроблене програмне забезпечення аналізу електромагнітної сумісності РЕЗ спеціального призначення.

Розроблене ПЗ призначене для:

– ведення бази даних радіоелектронних засобів (РЕЗ);

– розрахунку можливого взаємного можливого впливу РЕЗ з урахуванням рельєфу місцевості;

– відображення та аналіз даних щодо функціонування РЕЗ з використанням електронних карт місцевості.

Програмне забезпечення функціонує під управлінням операційних систем Windows та побудовано за архітектурою “клієнт-сервер”, що дозволяє створювати та накопичувати централізовану базу даних РЕЗ та використовувати її при проведенні розрахунків ЕМС.

Розрахункові модулі розроблені відповідно розроблених методик, в основу яких покладені рекомендації Міжнародного союзу електрозв’язку.

ВИСНОВКИ

Проведений аналіз спеціалізованого програмного забезпечення для планування бездротових мереж зв’язку показав що, максимальні необхідні можливості надає спеціалізоване програмне забезпечення виробництва компанії ATDI - ICS Telecom. Таким чином функціонал зазначеного СПЗ найбільш доцільно взяти за основу при створенні інформаційної системи ведення реєстрів радіоелектронних засобів спеціального призначення та розрахунку їх електромагнітної сумісності.

к.т.н. Гурський Т.Г. (ВІТІ)

ПІДВИЩЕННЯ ЗАВАДОЗАХИЩЕНОСТІ ПОВІТРЯНИХ РЕТРАНСЛЯТОРІВ УКХ РАДІОМЕРЕЖ В УМОВАХ НАВМИСНИХ ШУМОВИХ ЗАВАД

В останні десятиліття у арміях різних держав активно використовуються безпілотні літальні апарати (БЛА). Основним їх призначенням є ведення розвідки. У той же час, перспективним напрямком бойового застосування БЛА є розміщення на їхній платформі малогабаритних ретрансляторів для наземних УКХ радіомереж [1, 2].

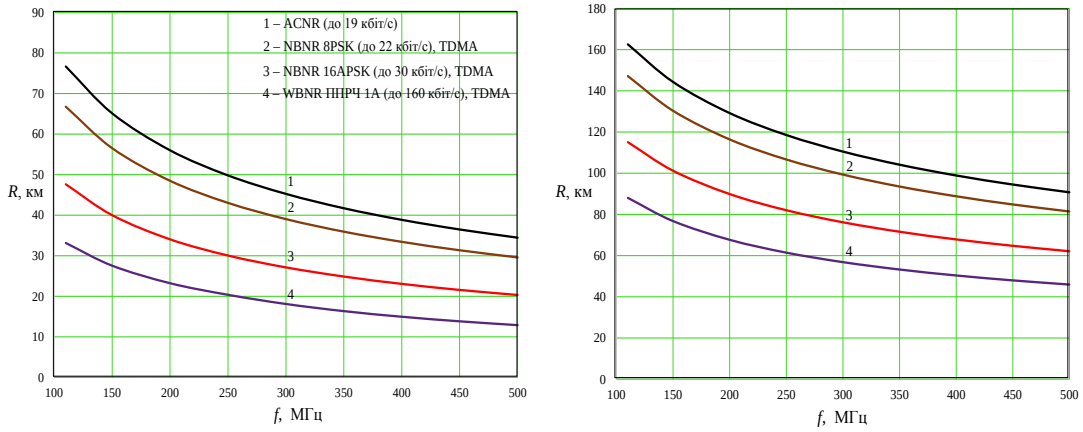
Переваги застосування повітряних ретрансляторів (радіостанцій) на БЛА очевидні:

значне збільшення зони покриття, порівняно з наземними ретрансляторами;

підвищення зв'язності радіостанцій мережі;

можливість гнучкого оперативного управління топологією мережі шляхом переміщення БЛА, на відміну від радіомереж з наземними ретрансляторами (НР).

На рис. 1 показано розрахунки дальності зв'язку у різних режимах роботи між радіостанціями PRC-9661 (виробництва Aselsan) потужністю 10 Вт, проведені у роботі [3], одна з яких – наземна з висотою підвісу антени 2,2 м, інша – з антеною на щоглі висотою 30 м, що відповідає НР (рис. 1, *а*), або розташована на БЛА на висоті 200 м (рис. 1, *б*). Розрахунки проводились з використанням моделі Хата для відкритої (сільської) місцевості. Видно, що при використанні ПР дальність зв'язку збільшується у 2 – 3 рази в залежності від режиму роботи та робочої частоти, порівняно з мережею з НР (рис. 2). Для умов міста та тих же вихідних даних різниця ще більша (у 3 – 4 рази) [3].



а) *б*)

Рис. 1. Орієнтовна дальність зв'язку між радіостанціями PRC-9661 для відкритої місцевості:
а) при h_1 = 30 м, h_2 = 2,2 м; б) при h_1 = 200 м, h_2 = 2,2 м

Збільшення висоти польоту повітряного ретранслятора (ПР) дозволить збільшити зону покриття (або, при однаковій дальності зв'язку, зменшити необхідну потужність передавача, що, в першу чергу, дозволить подовжити час безперервного польоту БЛА).

Радіостанції (ретранслятори) різних виробників, які можуть встановлюватися на БЛА, наведені у табл. 1.

Згідно із заявленими виробником даними виріб Agent-201 забезпечує радіус зони покриття до 70 км при підйомі на висоту 600 м, виріб Agent-202, який представляє собою ретранслятор SLR5500, виконаний у спеціальному корпусі для встановлення на повітряних об'єктах, забезпечує радіус зони покриття до 130 – 150 км при підйомі на висоту 600 м.

На сьогоднішній день компанія Aselsan не випускає спеціального обладнання для встановлення на БЛА та ін. аероплатформах. Випускається авіаційна радіостанція VRC-9681, яка дещо легша за VRC-9661, проте, на відміну від неї, не підтримує мережеві (Ad Hoc) режими – NBNR та WBNR). Найлегша – портативна радіостанція PRC-9651 не підтримує широсмуговий високошвидкісний режим WBNR. Тому важливим завданням є замовлення

(розробка) малогабаритних радіостанцій Aselsan для встановлення на телекомунікаційних аероплатформах.

Таблиця 1

Обладнання УКХ радіозв'язку для створення ретрансляторів на базі аероплатформ

Виробник	Ретранслятор	Потужність , Вт	Габарити (ВхШхД), мм	Вага (без антен)
Motorola	Agent-202 (SLR-5500)	1-45	72x205x375	4,8
	Agent-202 з дуплексером	1-45	105x205x410	5,9
	Agent-201 (2xDP4400)	1; 5	55x58x160	0,48
Harris	RF-7850A-UA	10	8,13x13,46x4,44	0,635
Aselsan	VRC-9681	30 (ЧМ) 10-15 (ACNR)	150x240x130	7
	PRC-9651	0,1; 1; 4 (ACNR) 1; 2 (NBNR)	85x257x54	1,4
	PRC-9661	1; 5; 10 (ACNR, NBNR, WBNR)	240x247x96	4,75

Слід зазначити, що у режимах ACNR (Aselsan), FF та усіх різновидах ППРЧ – Quicklook (Harris), для конфігурації ретранслятора необхідно 2 радіостанції. У той же час, у режимах роботи з підтримкою MANET (NBNR, WBNR для Aselsan та ANW2 для Harris) на борту БЛА має бути одна радіостанція [4], яка, за рахунок значної висоти підйому БЛА, може мати пряму радіовидимість з усіма іншими радіостанціями мережі та забезпечувати їх зв'язність. В літературі велику увагу приділено розробці та розвитку методів підвищення пропускної спроможності та зв'язності радіомереж з повітряними ретрансляторами на БЛА [1]. У той же час, проблема забезпечення завадозахищеності таких радіомереж залишається розв'язаною тільки частково [5].

Відомо [6], що для забезпечення можливості передачі інформації у різних режимах роботи (для різних сигнально-кодових конструкцій) необхідно забезпечити відношення сигнал/завада (ВСЗ) від декількох одиниць (низькошвидкісна передача даних (ПД), короткі текстові повідомлення, голос) до понад двадцяти (високошвидкісна ПД). Для оцінки впливу засобів радіоелектронної боротьби (РЕБ) на радіомережі з ретрансляторами необхідно, в першу чергу, розрахувати очікуване ВСЗ на входах приймачів (ретрансляторів та радіостанцій). Розрахунки рівнів корисного сигналу та навмисної завади на входах приймачів здійснюються з рівняння радіолінії. Для розрахунку втрат при розповсюдженні радіохвиль, в залежності від вихідних даних, можна скористатися моделлю Хата, формулою Введенського, рекомендацією ITU-R P.1546, моделлю вільного простору або іншими відомими методиками [5].

У роботі [5] розглянуто вплив засобів радіоелектронної боротьби (РЕБ), як потужних наземних, так і малопотужних повітряних (на БЛА), на радіомережі двох типів (з наземними та повітряними ретрансляторами), що працюють у режимі ППРЧ. Встановлено, що завадозахищеність радіомережі з ПР в цілому вища, порівняно з радіомережею з НР, проте ПР на БЛА, розташований на значній висоті, є зручною ціллю для потужних наземних засобів РЕБ. Результати розрахунків очікуваного ВСЗ на вході приймача ПР в залежності від відстані між ретранслятором та радіостанцією, проведених в [5] для типових технічних характеристик радіостанцій та наземного ПЗ, що формує шумову загороджувальну завади (ШЗЗ), представлені на рис. 2.

Відомо, що ефективність постановки шумових завад можна підвищити за рахунок не повного, а часткового перекриття хопсету, але з більшою спектральною щільністю потужності [6, 7]. Таку заваду називають шумовою завадою в частині смуги (ШЗЧС). Тому, в залежності від виду модуляції (сигнально-кодової конструкції), що використовується у

обраному режимі роботи, можна розрахувати оптимальну стратегію постановника шумової завади в частині смуги та, відповідно, ймовірність бітової помилки на найгірший випадок.

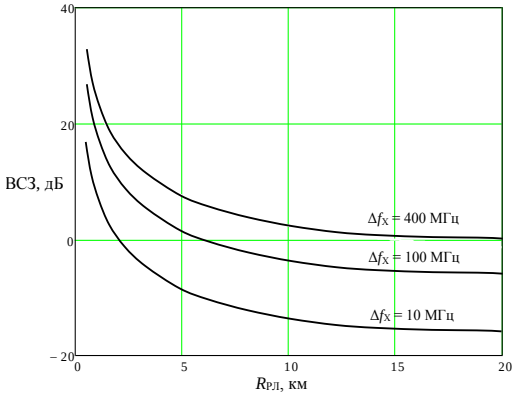


Рис. 2. Очікуване ВСЗ на вході приймача ПР

На рис. 3 для прикладу наведено графіки залежності ймовірності бітової помилки для двійкової фазової маніпуляції (ФМ-2) від відношення сигнал/шум для різних значень коефіцієнта перекриття ШЗЧС γ [5]. В табл. 2 наведено відповідні значення γ.

Таблиця 2

γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	γ_8	γ_9	γ_{10}
0,0001	0,0005	0,001	0,005	0,01	0,05	0,1	0,3	0,5	1

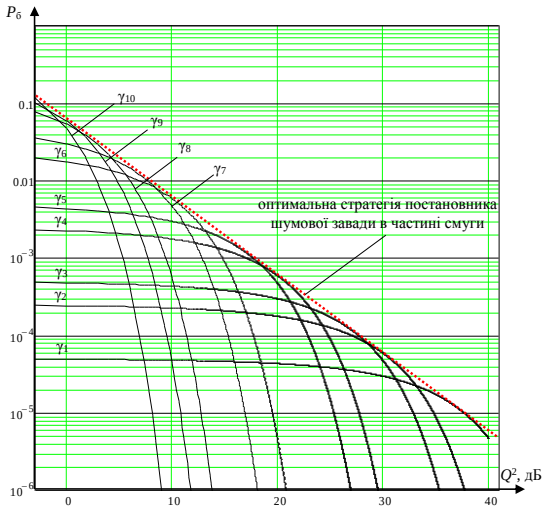


Рис. 3. Завадостійкість радіолінії з ППРЧ та ФМ-2 при впливі ШЗЗ та ШЗЧС

Розглянемо приклад. Нехай наземний ПЗ подавлює приймач ПР, який знаходиться на віддаленні 4 км від радіостанції та, відповідно, 14 км від ПЗ, і працює з шириною хопсета 400 МГц. При цьому ПЗ досягає ВСЗ близько 10 дБ при постановці ШЗЗ (рис. 2) та, відповідно, для ФМ-2 $P_б = <10^{-6}$ (рис. 3), але оптимальним значенням коефіцієнта перекриття, як видно з рис. 3, є $\gamma_7 = 0{,}1$. При цьому отримаємо $P_б = 6 \cdot 10^{-3}$.

Враховуючи, що засоби РЕБ формують шумові завади з дискретним перемиканням ширини смуги, ПЗ у більшості випадків не буде формувати оптимальну заваду, проте може обрати найбільш ефективне значення ширини її смуги.

При ширині каналу 1 МГц ВСЗ зменшується приблизно на 16 дБ (вигляд графіків такий же самий, як на рис. 2) [5]. Крім того, для забезпечення необхідної достовірності передачі інформації у широкосмуговому режимі необхідно набагато більше відношення сигнал/(шум + завада). Отже, завадозахищеність широкосмугового режиму роботи значно менша.

Отримані залежності очікуваного ВСЗ на вході приймача ПР та графіками завадостійкості при впливі ШЗЧС дозволяють на етапі планування (проектування радіомережі) на основі даних про характеристики засобів РЕБ та їх розташування визначати максимально допустиме віддалення ПР від наземних радіостанцій (фактично – максимальне покриття ПР) для забезпечення заданого відношення сигнал/завада.

Очевидно, що для підвищення завадозахищеності ПР необхідно збільшувати ширину хопсета та зменшувати дальність радіоліній за рахунок наближення ретранслятора до радіостанцій (а отже – зменшення радіусу зони покриття, що не завжди є прийнятним). Тому необхідно вживати додаткових заходів для підвищення завадозахищеності, особливо у широкосмуговому режимі. В роботі [8] зазначено, що з погляду ослаблення сигналу завади на вході приймача, при визначенні висоти та траєкторії баражування ПР на БЛА необхідно враховувати характеристики спрямованості його антени, а також здійснювати аналіз місцевості (побудову профілю, сукупності профілів між точкою знаходження БЛА та точкою встановлення антени ПЗ) з метою використання її захисних властивостей. Графіки ВСЗ на рис. 2 отримані для значення коефіцієнта підсилення антени ПР 0 дБі, як у напрямку на радіостанцію, так і у напрямку на ПЗ. Очевидно, що за рахунок зменшення коефіцієнта підсилення антени у напрямку на джерело завад ВСЗ збільшиться.

Розглянемо радіолінію з ПР на БЛА, яка складається з двох радіостанцій і ПР (рис. 4). Нехай $РС_1$ та $РС_2$ – найбільш віддалені радіостанції у радіомережі. При цьому, залежності кута підйому антени ПР $\psi_{ПР}$ та кута місця антени радіостанції $\beta_{РС}$ від дальності зв'язку R_i та висоти підйому БЛА h визначаються з наступних виразів [9]:

$$\psi_{ПР}^{\circ} = \arctan\left(\frac{\sin\left(\frac{R_i}{R_з}\right)}{1+\frac{h}{R_з}-\cos\left(\frac{R_i}{R_з}\right)}\right)\cdot\frac{180}{\pi};$$

$$\beta_{РС}^{\circ} = \left(\arctan\left(\frac{1+\frac{h}{R_з}-\cos\left(\frac{R_i}{R_з}\right)}{\sin\left(\frac{R_i}{R_з}\right)}\right)-\frac{R_i}{R_з}\right)\cdot\frac{180}{\pi},$$

де $R_з$ – радіус земної сфери. Очевидно, що ширина діаграми направленості антени (ДНА) ПР у вертикальній площині повинна бути не меншою за подвоєне значення кута підйому антени ПР: $2\Delta\theta_{0,5}^{\circ} \geq 2\psi_{ПР}$.

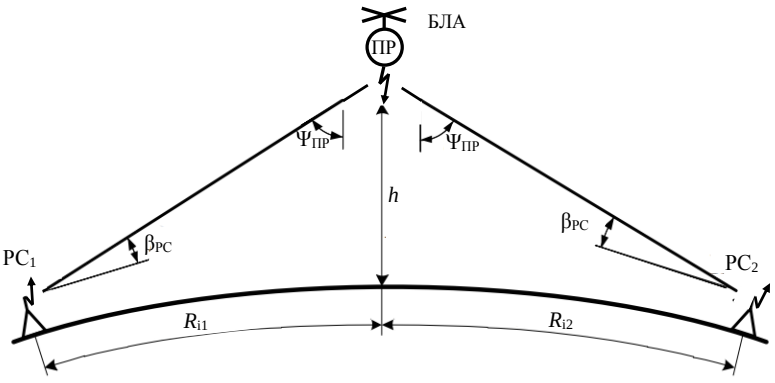


Рис. 4. Геометрична інтерпретація радіолінії з ретрансляцією через БЛА

Зазвичай для наземної радіостанції кут місця $\beta_{РС}$ лежить у межах від 5° до 90°, а в умовах щільно забудованого міста – від 60° [1], проте для діапазону робочих частот військових УКХ радіозасобів ці вимоги можуть бути менш жорсткими.

Таким чином, знаючи відстані до найбільш віддалених радіостанцій та ширину ДНА ПР можна визначити мінімально необхідну висоту підйому БЛА ПР, при якій буде забезпечуватись заданий коефіцієнт підсилення антени.

Слід розуміти, що наведені вирази виведені за умови забезпечення прямої видимості між антенами ПР та РС, якщо прийняти, що Земля є ідеальною сферою з радіусом 6370 км. Реальна дальність зв'язку може бути більшою за рахунок дифракції (огинання радіохвилями земної поверхні), а також за рахунок того, що при перевищенні кута підйому значення $\psi_{ПР}$, коефіцієнт підсилення антени зменшується поступово. Робота на більш низьких частотах також призведе до збільшення дальності зв'язку.

На рис. 5 наведено залежність необхідних значень кута підйому антени ПР $\psi_{ПР}$ (рис. 5, а) та кута місця антени наземної радіостанції $\beta_{РС}$ (рис. 5, б) від дальності зв'язку між ПР та РС (R_i) для висоти підйому ПР h від 200 до 4000 м (числа над графіками відповідають висоті польоту БЛА h, км).

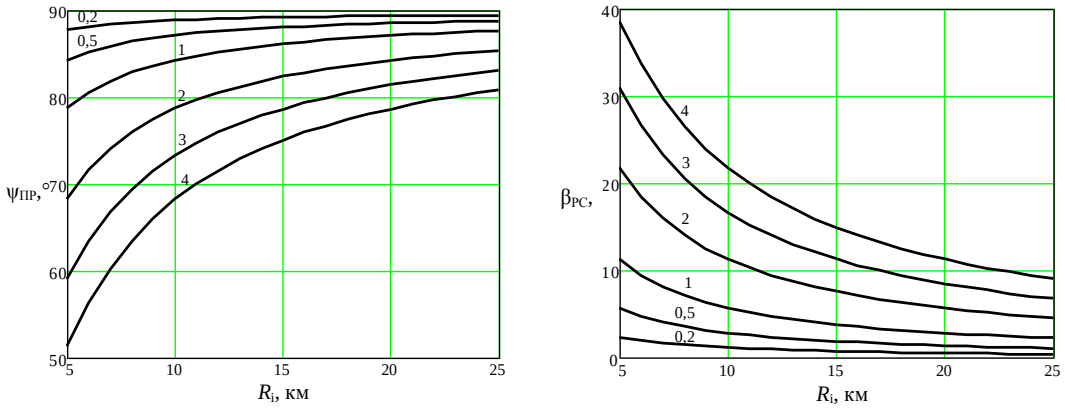


Рис. 5. Залежність кута підйому антени ПР $\psi_{ПР}$ та кута місця антени наземної радіостанції від дальності зв'язку R_i

Видно, що, наприклад, для забезпечення дальності зв'язку між радіостанцією та ПР 10 км та при $\psi_{ПР} = 80°$ необхідно піднімати БЛА на висоту близько 1750 м.

Для забезпечення максимального покриття антена ПР повинна володіти випромінюванням у нижню півсферу та забезпечувати $\psi_{ПР}$ до 90° (в ідеальному випадку – з шириною основного пелюстка у вертикальній площині, що наближається до 180°). У якості такої антени може бути використаний вертикальний несиметричний вібратор (ВНВ) над металевим екраном скінченних розмірів у формі круга з радіусом R_e, перевернутий верхнім кінцем у напрямку Землі. Вигляд діаграми направленості чвертьхвильового ВНВ у вертикальній площині в залежності від розміру екрана показано на рис. 6 [10].

Недоліками застосування такої антени на ПР є наступні:

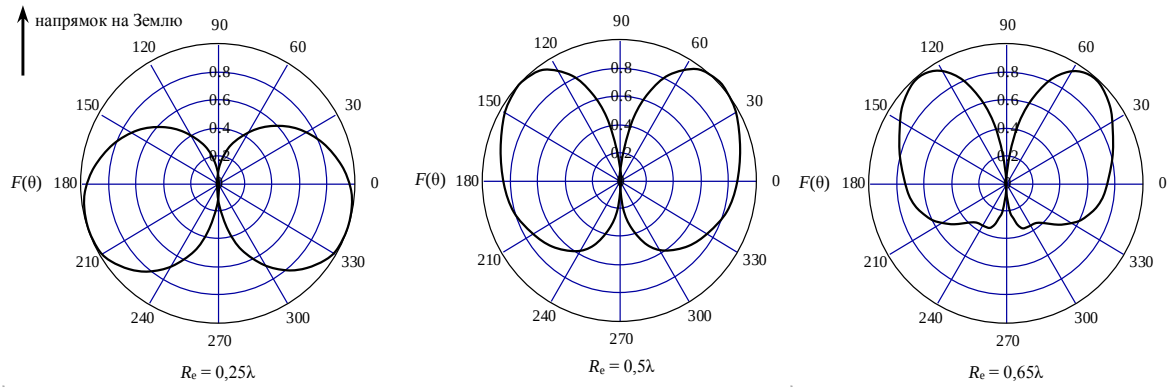
можливість існування „мертвої зони" під ПР, розміри якої будуть зростати при збільшенні висоти польоту БЛА;

геометричні розміри екрана (радіус) повинні бути досить значними (не менше половини довжини хвилі λ);

достатньо високий коефіцієнт підсилення у площині, перпендикулярній осі вібратора, що призведе до значного підсилення завади на вході приймача ПР.

У той же час, при величині $\psi_{ПР} < 90°$ є можливість обрати положення ПР таким чином, щоб засоби РЕБ противника знаходились поза межами основного пелюстка діаграми направленості антени. Такою антеною може бути низькопрофільна антена (НПА), проте вона значно менш широкосмугова, порівняно зі штирьовою [11], що потрібно враховувати при плануванні хопсетів. Відомо, що можна досягнути значень широкосмуговості НПА до 10% відносно центральної частоти. Довжина випромінюючого елемента (ВЕ) НПА повинна

складати λ/2, проте її можна зменшити у 2 – 4 рази (в $1/\sqrt{\varepsilon'}$ рази, де ε' – відносна діелектрична проникність діелектрика, розташованого між ВЕ та екраном).



а) *б*) *в*)

Рис. 6. Діаграма направленості чвертьхвильового ВНВ у вертикальній площині в залежності від розміру екрана: *а*) $R_e = 0{,}25\lambda$; *б*) $R_e = 0{,}25\lambda$; *в*) $R_e = 0{,}25\lambda$

Враховуючи геометричні розміри антени, доцільно планувати роботу радіомереж з використанням ПР у верхній частині діапазону робочих частот (приблизно від 200 – 300 МГц і вище) з урахуванням вантажопідйомності та габаритів БЛА. При цьому, оскільки НПА є досить вузькосмуговою, ПР повинен комплектуватися набором з декількох антен з можливістю їх заміни перед його розгортанням (запуском БЛА).

Перевагами НПА, порівняно з ВНВ, є наступні:

відсутність „мертвої зони” під ПР;

можливість забезпечення просторової фільтрації завади за рахунок направлених властивостей антени (забезпечення $\psi_{ПР} < 90°$).

Крім того, НПА може бути реалізована як з лінійною, так і з круговою поляризацією поля випромінювання.

Вигляд ДН НПА у вертикальній площині наведено на рис. 7. Форму (ширину) ДН НПА можна змінювати вибором розмірів випромінюючого елемента та екрана [11].

Рис. 7. Діаграма направленості НПА у вертикальній площині

Ще одним варіантом антенної системи ПР, яку можна використати для встановлення на БЛА, є фазовані антенні решітки (ФАР) [11], проте їх геометричні розміри, навіть у верхній частині діапазону робочих частот УКХ радіозасобів (300 – 512 МГц) можуть потребувати БЛА значних розмірів та вантажопідйомності. Наприклад, розрахунки, проведені в [9], показали, що для забезпечення ФАР з лінійними розмірами не більше 30х40 см, з шириною променя 6° та сектором сканування 60°х60°, діапазон частот має бути не менше 4 ГГц. Крім цього, застосування антен типу ФАР зі скануванням зони обслуговування призведе до необхідності удосконалення множинного доступу.

Тому для діапазону робочих частот військових УКХ радіозасобів доцільно застосовувати ненаправлені у горизонтальній площині антени з випромінюванням у нижню півсферу та шириною ДН у вертикальній площині не менше 140° (при такому значенні для забезпечення радіусу зони покриття (R_i) не менше 10 км висота польоту БЛА повинна складати 4000 м (рис. 4, 5)).

Очевидно, що одним із важливих завдань, як при реалізації просторової фільтрації завад за рахунок раціонального вибору просторового положення ПР, так і при забезпеченні необхідної зони покриття, є стабілізація його положення (положення антени ретранслятора) у вертикальній площині. Чим більшою буде похибка $\Delta\psi_{ПР}$, тим більший запас зони покриття необхідно забезпечувати, порівняно з необхідною, і тим складніше забезпечити просторову фільтрацію завади. Це завдання може бути вирішене алгоритмами управління антенною системою, які повинні компенсувати просторову нестабільність БЛА. Такі алгоритми можуть бути реалізовані за рахунок реалізації наступних підходів [9]:

гіростабілізованих платформ (ГСП);

сервоприводів наведення АС;

антенних систем з електричним скануванням.

Останні два підходи доцільно реалізовувати при використанні вузькоспрямованих антенних систем та антенних решіток. Тому при використанні антен типу ВНВ або НПА найбільш доцільним є використання ГСП.

Таким чином, основними етапами процедури позиціонування повітряного ретранслятора на БЛА в умовах активної радіоелектронної протидії є наступні:

1) введення вихідних даних: тип радіостанцій та повітряного ретранслятора та їх технічні характеристики (режим роботи, потужності передавачів та чутливості приймачів, коефіцієнти підсилення антен, їх характеристики (діаграми) направленості робочі частоти, (хопсети) на передачу та прийом); зона покриття (область, задана координатами можливого знаходження радіостанцій); координати розміщення станції (станцій) РЕБ, їх технічні характеристики (тип завади, потужність передавача, кількість літер та ширина їх частотних смуг, коефіцієнт підсилення антени);

2) визначення геометричного центру зони покриття;

3) визначення висоти підйому БЛА, при якій для заданої ДНА ПР забезпечується покриття необхідної зони (з урахуванням необхідності виконання умови $2\Delta\theta^{\circ}_{0,5} \geq 2\psi_{ПР}$). На цьому етапі можливе коригування координат розміщення (траєкторії баражування) БЛА з урахуванням рельєфу місцевості;

4) енергетичний розрахунок рівня сигналу ПР на границі зони покриття. У випадку надлишкового енергетичного запасу приймається рішення на зменшення потужності передавача ПР;

5) енергетичний розрахунок радіоліній ПЗ – ПР та РС – ПР (з урахуванням значень коефіцієнта підсилення антени ПР у напрямках на станцію РЕБ та РС). Розрахунок значення відношення сигнал/завада на вході приймача ПР;

6) розрахунок завадостійкості приймання інформації для випадку оптимальної (найбільш ефективної) ШЗЧС.

Якщо у випадку найгіршої завади ймовірність бітової помилки не перевищує допустиме значення, розрахунок закінчується. Якщо завадостійкість незадовільна – змінюються координати ПР таким чином, щоб зменшити значення коефіцієнта підсилення його антени у напрямку ПЗ настільки, щоб ВСЗ стало задовільним. Це можна реалізувати або зменшенням висоти польоту БЛА (при цьому погіршиться покриття на границі усієї зони обслуговування) або віддаленням БЛА від ПЗ (погіршиться покриття радіостанцій, які знаходяться ближче до противника). Іншим шляхом підвищення значення ВСЗ є збільшення, якщо це можливо, ширини хопсету з урахуванням частотної характеристики антени та вимог до електромагнітної сумісності з сусідніми радіомережами). Таким чином, повторюється виконання пунктів 3 – 6.

Якщо ж забезпечити покриття необхідної зони не вдається, для режимів роботи з підтримкою Ad-Hoc може застосовуватись декілька повітряних ретрансляторів. У той же час, у таких мережах відсутність зв'язку з деякими станціями радіомережі на границі необхідної зони покриття з великою ймовірністю не призведе до їхньої ізоляції завдяки ретрансляції через сусідні наземні радіостанції.

На етапі оперативного управління топологією мережі координати ретранслятора можуть уточнюватись з урахуванням переміщення наземних радіостанцій.

Висновки. Таким чином, повітряні ретранслятори на БЛА в УКХ радіомережах, порівняно з наземними радіостанціями, можуть бути значно ефективніше подавлені потужними наземними засобами РЕБ. Основними заходами підвищення завадозахищеності, запропонованими у роботі, є застосування режиму ППРЧ з достатньо великим значенням ширини смуги частот (хопсету) та просторова фільтрація завад за рахунок вибору висоти баражування та віддалення від постановника завад з урахуванням необхідності забезпечення покриття заданої зони обслуговування. Забезпечити ослаблення завади на вході приймача повітряного ретранслятора в діапазоні робочих частот військових УКХ радіозасобів може низькопрофільна антена. При цьому, вибір параметрів (ширина хопсету та координати польоту) здійснюється на основі попередньо розрахованих значень очікуваного відношення сигнал/завада на вході приймача повітряного ретрнаслятора та ймовірності бітової помилки на найгірший випадок (при постановці оптимальної шумової завади в частині смуги).

ЛІТЕРАТУРА

1. Романченко І.С. Моделі застосування інформаційно-телекомунікаційних технологій на основі безпілотних авіаційних комплексів у надзвичайних ситуаціях: монографія / І.С. Романченко, С.Л. Данилюк, С.М. Чумаченко [та ін.]. – К.: НАУ, 2016. – 332 с.
2. Літаючі самоорганізуючі радіомережі / [В.А. Романюк, Є.О. Степаненко, І.В. Панченко, О.І. Восколович] // Збірник наукових праць ВІТІ. – 2017. – № 1. – С. 104 – 114.
3. Гурський Т.Г. Оцінка граничної дальності зв'язку на сучасних радіо- та радіорелейних лініях / Т.Г. Гурський, Є.О. Степаненко, А.В. Шишацький // Збірник наукових праць ВІТІ. – 2019. – № 1. – С. 6 – 17.
4. Аналіз режимів роботи та перспектив бойового застосування військових УКХ радіостанцій іноземного виробництва / [Кувшинов О.В., Гурський Т.Г., Гриценок К.М., Шишацький А.В.] // Збірник наукових праць ВІТІ. – 2018. – № 1. – С. 43 – 50.
5. Гурський Т.Г. Аналітична модель оцінки впливу засобів РЕБ на радіолінії з ППРЧ у радіомережах з повітряним та наземним ретрансляторами / Т.Г. Гурський // Збірник наукових праць ВІТІ. – 2019. – № 3. – С. 23 – 32.
6. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.: пер. с англ. / Б. Скляр. – М.: Издательский дом „Вильямс", 2007. – 1104 с.
7. Борисов В. И. Помехозащищенность систем радиосвязи. Вероятностно-временной подход. Изд. 2-е, исправленное / В. И. Борисов, В. М. Зинчук.– М.: „Радиософт", 2008. – 260 с.
8. Аналіз завадозахищеності радіомереж з використанням повітряних ретрансляторів в умовах навмисних шумових завад / [Гурський Т.Г., Сова О.Я., Гриценок К.М., Гай Ю.І.] // Збірник наукових праць ВІТІ. – 2018. – № 4. – С. 26 – 33.
9. Алешин М.Г. Обоснование основных характеристик антенной системы и параметров управления мощностью передатчика ретранслятора связи на беспилотном летательном аппарате / М. Г. Алешин, С. В. Дьяконов, А. Ю. Сивов // Журнал радиоэлектроники. – № 12. – 2011. – 21 с.
10. Резников Г. Б. Антенны летательных аппаратов / Г.Б. Резников. – М.: „Советское радио", 1967. – 416 с.
11. Balanis C.A. Antenna Theory: Analysis and Design / C.A. Balanis. – John Wiley & Sons, Inc., 2016. – 1095 p.

к.т.н. Давіденко С.В. (НАСВ)
Бойчук Б.М. (НАСВ)

ПРИНЦИПИ КОНВЕРГЕНЦІЇ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Сучасному періоду розвитку телекомунікації відповідає зростання попиту на телекомунікаційні послуги та чітко прослідкується тенденція швидкого зростання об'ємів трафіку даних на телекомунікаційних мережах. Поступово трафік даних стає домінуючим, що вимагає створення телекомунікаційних мереж з високою пропускною здатністю на базі комутації пакетів. Збільшується кількість користувачів, як в повсякденній, так і в професійній діяльності, разом з традиційними послугами зв'язку, яким потрібні послуги передачі даних і доступу в Інтернет. Зростає мультимедійниий трафік у телекомунікаційних мережах на основі IP- технологій.

З метою забезпечення обслуговування зростаючого мультимедійного трафіку проводиться модернізація існуючих і будівництво нових мереж, що приводить до поступового переходу до конвергентних мереж, яка може бути розділена на мережеву конвергенцію, конвергенцію сервісів, конвергенцію терміналів, промислову (індустріальну) конвергенцію

Першим кроком на шляху конвергенції телекомунікаційних мереж є оптимізація транспортної мережі для покращення надання мовних послуг.

Другим кроком є нарощування продуктивності транспортної мережі для надання нових мультисервісних послуг і використання технології ALL-IP.

Технологічно конвергенція телекомунікаційних мереж здійснюється на базі стека протоколів TCP/IP, як в мережі радіодоступу, так і в транспортній мережі.

В той же час існує ряд труднощів і перешкод на шляху повномасштабної реалізації конвергенції телекомунікаційних мереж, а саме: складність створення транспортної системи з високою швидкістю передавання різнорідного трафіку; достатньо висока складність конвергованого абонентського обладнання; технічна недосконаліть дворежимних терміналів (WLAN/мобільний зв'язок); часта відсутність технічних можливостей оптимізації передавання голосового трафіку в конвергованих мережах; обмеженість кількості рішень конвергенції фіксованих та мобільних мереж; необхідність здійснення управління дворежимними послугами фіксованих-мобільних операторів та інше.

Виходячи з цього транспортна платформа конвергентних мереж повинна бути широкосмуговою мультисервісною мережею, яка забезпечує передавання будь-яких видів трафіку з підтримкою необхідної якості сервісу.

На сьогодні побудова лінійних трактів конвертованих мереж базується на використанні технології DWDM (Dense Wavelength Division Multiplexing – ущільнене мультиплексування з розділенням по довжині хвилі). В лінійних трактах кожна оптична хвиля утворює віртуальний канал, який в подальших елементах транспортної мережі мультиплексується. На вузлах мультиплексування відбувається комутація по довжині хвилі з можливістю вводу виводу зовнішніх потоків. Тому влив параметрів вузлів комутації і мультиплексування є суттєвим і ці параметри повинні бути враховані у моделях. Передавання даних з використанням декількох оптичних хвиль і подальша комутація та мультиплексування утворює кільцеві топології, які поєднуються у вузлах, які складають основу фундаменту трансформації традиційних мереж загального користування з комутацією каналів в конвергентні мережі наступного покоління (NGN).

Таким чином конвергенція телекомунікаційних мереж забезпечить реалізацію загальних архітектурних принципів телекомунікаційних мереж, підтримку єдиних сумісних протоколів апаратно-програмних засобів телекомунікації, реалізацію єдиних підходів до використання телекомунікаційних технологій і надання телекомунікаційних послуг та дозволить реалізувати велику кількість нових телекомунікаційних послуг типу „людина-людина", „людина-контент" і „контент-людина" .

Давидов А.А. (НУОУ)

ВИЗНАЧЕННЯ ПОКАЗНИКА ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ РАДІОСВІТЛОТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ ТАКТИЧНОЇ АВІАЦІЇ В РАЙОНІ АЕРОДРОМУ

Актуальність, постановка задачі. Зліт, політ в районі аеродрому та посадка є обов'язковими етапами польоту повітряного судна. З метою забезпечення польотів на цих етапах польоту на аеродромах створюється система радіосвітлотехнічного забезпечення. Наявність мети функціонування системи радіосвітлотехнічного забезпечення польотів тактичної авіації в районі аеродрому дозволяє стверджувати, що її функціонування це операція, тому виникає потреба в оцінюванні її ефективності.

Мета. Визначити показник ефективності функціонування системи радіосвітлотехнічного забезпечення в районі аеродрому.

Основні положення. Одним з часткових показників, за яким визначають придатність до експлуатації аеродромів є мінімум аеродрому [1]. Він характеризує метеорологічні умови при яких системою радіосвітлотехнічного забезпечення забезпечується безпечна посадка повітряного судна і характеризується граничними значеннями нижнього краю хмарності та дальністю прямої видимості. Для забезпечення необхідного мінімуму аеродрому відповідний напрямок злітно-посадкової смуги повинен бути обладнаний радіосвітлотехнічним обладнанням у стаціонарному або рухомому варіанті відповідно до „Складу радіотехнічного обладнання аеродрому державної авіації України" [1]. Мінімуми аеродромів під час заходу на посадку за приладами при різних варіантах посадкового радіо- та світлотехнічного обладнання наведено в [1]. Згідно методики визначення норм цілісності та безперервності обслуговування на основі методу дерева ризику ризик втрати літака внаслідок відмови системи, яка не знаходиться на борту повітряного судна обумовлюється порушенням цілісності основного наведення та порушення безперервності обслуговування [2]. Цілісність та безперервність обслуговування, як і мінімум аеродрому, залежать від кількості залучених до забезпечення посадки повітряного судна засобів радіосвітлотехнічного забезпечення, а мінімум аеродрому додатково визначає межу безпечного функціонування контуру управління процесом посадки повітряних суден. Це дає підставу визначення показником ефективності функціонування системи радіосвітлотехнічного забезпечення тактичної авіації в районі аеродрому її стійкість. Оскільки візуальне орієнтування має вагоме значення для забезпечення кінцевого етапу заходу на посадку, а установка радіонавігаційного засобу не усуває необхідності у візуальних засобах для забезпечення заходу на посадку та посадки в умовах обмеженої видимості [2], то радіонавігаційні засоби та світлотехнічне обладнання повинно застосовуватись комплексно. У цих умовах значення мінімуму аеродрому який забезпечується радіо маячною системою або радіолокаційною системою посадки в якості основних систем посадки рівні.

Висновок. В доповіді запропоновано підхід до вибору показника ефективності функціонування системи радіосвітлотехнічного забезпечення тактичної авіації в районі аеродрому, який дозволяє оцінювати ефективність її функціонування з урахуванням потреб тактичної авіації.

ЛІТЕРАТУРА

1. Правила визначення придатності до експлуатації аеродромів та злітно-посадкових майданчиків державної авіації України: Наказ Міністерства оборони України від 17 листопада 2014 р. № 811 / М-во оборони України. Київ: МО України, 2014 р.

2. Авиационная электросвязь (приложение 10 к Конвенции о международной гражданской авиации). В 5 т. / ИКАО – Квебек: ИКАО, 2006. Т. 1.

д.т.н. Демідов Б.О. (ХНУПС)
к.т.н. Капранов О.В. (ХНУПС)
к.т.н. Кучеренко Ю.Ф. (ХНУПС)
к.т.н. Ткачов А.М. (ХНУПС)

АВТОМАТИЗОВАНА СИСТЕМА УПРАВЛІННЯ МІЖВИДОВИМ УГРУПОВАННЯМ, ЯК ОДНА ІЗ СКЛАДОВИХ ОСНОВ ЙОГО БОЄЗДАТНОСТІ

На сучасному етапі розбудови Збройних Сил (ЗС) України велике значення приділяється розробці і впровадженню у війська, що будуються за стандартами НАТО, різних засобів (комплексів), а також систем з автоматизованого управління військами та зброєю, з метою підвищення ефективності управління частинами (підрозділами) багатофункціональних міжвидових угруповань військ (МУ).

Тому, вже зараз необхідне впровадження сучасної автоматизованої системи управління міжвидовим угрупованням (АСУ МУ), яка б забезпечила використання єдиного інформаційно-комунікаційного середовища (ЄІКС) всіма органами управління різних його формувань, з метою забезпечення набуття (отримання) інформаційної переваги над противником при веденні сучасних війн, які мають всі ознаки мережецентричних (інформаційних) війн.

Функціонування АСУ МУ, як взаємопов'язаної сукупності різних підсистем, повинно бути направлене на своєчасне і якісне вирішення всього комплексу інформаційних і розрахункових задач та моделей, з метою забезпечення максимального скорочення термінів циклів управління підпорядкованими військами і засобами та випередження у діях керівництва (органів управління) противника при прийнятті рішення в умовах динамічної зміни оперативної обстановки в зоні ведення бойових дій.

Боєздатність підрозділів МУ (що визначає можливості підрозділів даного угруповання військ вести воєнні (бойові) дії і виконувати поставлені завдання у відповідності до їх призначення та залежить від укомплектованості, бойової виучки і морально-психологічних якостей особового складу, бойових втрат і можливостей їх відновлення, забезпеченості озброєнням і військовою технікою й матеріальними засобами та інших чинників) у бою буде високою, якщо перед ними поставлена чітко визначена мета та визначені сили, засоби і способи дій підрозділів щодо досягнення заданої мети й організовано безперервне управління усіма підрозділами, що складають дане МУ за допомогою розгорнутої системи управління, яка при максимальному ступеню автоматизації буде відповідати АСУ МУ.

Тому основними складовими, що впливають на загальний стан боєздатності МУ при веденні сучасних (мережецентричних) війн слід вважати діяльність командирів і штабів, застосування особового складу, озброєння і техніки за єдиним задумом командування та надійне функціонування АСУ даного угруповання, а тому розглядання питання щодо АСУ МУ як однієї з складових основ боєздатності МУ при веденні сучасних бойових дій має дуже актуальне значення.

Певні підсистеми АСУ МУ відповідні за конкретні цикли управління військами, зброєю, інформаційними засобами, які визначаються їх призначенням і особливостями їх функціонування, а саме: різні інформаційні мережі (комплекси, засоби) визначають відповідні терміни циклів управління щодо збору інформації різних видів, її обробки та представлення органам управління і іншим підсистемам МУ вже реальної обстановки, що складається у зоні ведення бойових дій; системи підтримки прийняття рішень на основі аналізу динаміки зміни обстановки у зоні бойових дій здійснюють прогноз дій противника та визначають варіанти застосування своїх сил, на основі яких командир приймає рішення на постановку бойових завдань своїм частинам і за допомогою систем управління доводить їх до кожного підрозділу МУ; розвідувальні системи визначають термін виявлення цілі, її класифікацію та передачу відповідним користувачам, в тому числі і ударним системам усю необхідну інформацію про цілі; ударні системи у рамках свого циклу управління проводять

відповідні розрахунки щодо першочерговості знищення цілей, їх розподілу по засобам ураження, ставлять бойові завдання ударним комплексам, які знищують вказані цілі.

При веденні сучасних війн можливо спостерігати процес поступового зміщення акценту ведення збройної боротьби у інформаційну сферу, а тому вага системи управління та її вплив на інші складові боєздатності МУ на даний час значно зросла. У подальшому слід очікувати зростання ступеню автоматизації у різних підсистемах системи управління МУ ЗС до повної її автоматизації і створення інтегрованої АСУ МУ ЗС, що забезпечить комплексне застосування військ та їх бойових засобів за єдиним задумом і у реальному масштабі часу і її вплив на інші складові боєздатності МУ буде ще більшим .

Таким чином, можливо констатувати, що професіоналізм командирів та їх штабів – це інтелектуальна складова, яка впливає на зміну боєздатності військ МУ, а функціонування АСУ МУ – це інформаційна (інформаційно-інтелектуальна, при застосуванні елементів та технологій штучного інтелекту) складова, що впливає на забезпечення збереження та відновлення боєздатності МУ у процесі управління його підрозділами при застосуванні їх в сучасних бойових діях, оскільки повнота та своєчасність виконання відповідними органами управління своїх функціональних завдань залежить від якісного функціонування усіх інформаційних складових АСУ МУ, до того ж, вони забезпечують зменшення термінів циклів управління даними підрозділами, а також дозволяють здійснити комплексне використання основних складових боєздатності за єдиним задумом командування у відповідності до поставленим різним підрозділам МУ завданням, тим самим збільшують могутність даного угруповання по відношенню до іншого угруповання військ, яке немає у своєму складі таких інформаційних систем.

Чим вище ступінь автоматизації процесів управління частинами (підрозділами) МУ та їх бойовими засобами (за рахунок застосування багатоцільових комплексів засобів автоматизації, перспективних програмно-технічних комплексів, новітніх інформаційних технологій), тим більше їх бойові можливості, які збільшуються за рахунок комплексного та синхронізованого застосування військ та їх бойових засобів за єдиним задумом командування і у реальному масштабі часу, на основі використання органами управління можливостей ЄІКС в районі ведення бойових дій, яке формується відповідною АСУ МУ.

Комплексна автоматизація процесів управління МУ дає можливість суттєво зменшити цикли управління підпорядкованими військами і засобами за рахунок використання можливостей ЄІКС органами управління та своєчасно оцінювати обстановку і приймати рішення командирам відповідних рівнів управління на застосування військ у стислі терміни та у відповідності до зміни оперативно-тактичній обстановки в зоні ведення бойових дій. Оскільки кожна складова боєздатності має відповідний вплив на загальну боєздатність МУ, яка залежить від надійної взаємодії усіх своїх складових (дій особового складу, озброєння і техніки, та засобів матеріально-технічного забезпечення бойових дій) і в першу чергу дій органів управління, що визначається вмінням використовувати усі можливості ЄІКС, яке створюється відповідними складовими АСУ МУ, то у сучасних війнах АСУ МУ являється однією з головних складових боєздатності міжвидового угруповання.

Тому застосування перспективних АСУ МУ слід розглядати не тільки як засіб здійснення ефективного управління частинами та засобами МУ але і як основну складову їх боєздатності, даний факт необхідно враховувати при оцінки можливостей як противника, так і своїх військ щодо ведення сучасних бойових дій в різних умовах обстановки.

Дніпровська А.М. (ЦНДІ ОВТ ЗСУ)
к.т.н. Жук П.В. (НУОУ)

ПЕРСПЕКТИВНІ НАПРЯМКИ РОЗВИТКУ БАГАТОФУНКОНАЛЬНОЇ АВТОМАТИЗОВАНОЇ СИСТЕМИ РЕБ ЗБРОЙНИХ СИЛ УКРАЇНИ

Актуальність дослідження. Досвід проведення ООС доводить, що для противника української сторони характерне широке застосовання сучасних радіоелектронних та інформаційних технологій і створених на їх основі інформаційно-керуючих систем різного призначення. У зв'язку з цим, перед Збройними Силами (ЗС) України постає актуальне завдання пошуку інноваційних схем і методів ведення радіоелектронної боротьби (РЕБ).

Постановка завдання дослідження. В процесі планування застосування засобів та сил РЕБ вирішується низка інформаційно-розрахункових задач, що потребує збору та обробки великої кількості вихідних даних. Одним із шляхів вирішення даного питання є підвищення ефективності застосування сил та засобів РЕБ шляхом автоматизації найбільш складних і трудомістких процесів планування та управління зазначеними системами з подальшою розробкою і впровадженням елементів багатофункціоальної автоматизованої системи управління (АСУ) РЕБ.

Основні положення. На сьогодні у збройних силах США питанням автоматизації основних процесів управління підрозділами РЕБ приділяється увага провідних країн світу. Розробка сучасної апаратури РЕБ ведеться за програмою „Prophet", а також проекту „WolfPack", в рамках якого створено принципово нову інтегровану АСУ РЕБ IEWS, що об'єднує усі наземні та повітряні засоби РЕБ та забезпечує вирішення широкого кола задач в діапазоні 20 – 15000 МГц.

Створення універсальних АСУ РЕБ визначено головним напрямом розвитку військ і Російською Федерацією (РФ). Одне з останніх досягнень РФ – багатофункціональний мобільний комплекс "Дивномор'є", головна перевага якого – повна автоматизація. Ще одна інновація – комплекс "Палантин", у якому реалізована сучасна система підтримки прийняття рішень, що вибудовує оптимальний алгоритм виконання завдань, автономно розподіляє ресурси і функціональне навантаження кожної з підсистем.

В основу проектування таких систем покладено мережоцентричні методи радіоелектронної розвідки (РЕР), управління РЕБ і всебічного забезпечення. Такий підхід забезпечує високу адаптованість систем до змін радіоелектронної обстановки (РО), скорочення тривалості циклів і підвищення стійкості управління.

Завдання моніторингу та розпізнавання радіосигналів в таких системах вирішується застосуванням програмно визначених радіосистем (SDR), що дозволяє передавати і обробляти сигнали з використанням різних частот і стандартів, а усі параметри пристрою визначаються програмно. Така технологія дозволяє на рівні програмного забезпечення (ПЗ) реалізувати багаторежимність, багатодіапазонність, скритність від РЕР супротивника.

Для вирішення радіоелектронного конфлікту між системою радіозвязку та системою радіоелектронного подавлення, який характерний для систем РЕБ використовується режим псевдовипадкового перестроєння робочої частоти (ППРЧ).

Розпізнавання цілей забезпечується одночасно різними способами (повнокадрове відео, електронно-оптичні сенсори, ІЧ-сенсори, прив'язка джерел радіовипромінювання до місцевості та ін.). Ці системи разом з моделями загального призначення і вдосконаленими розвідувальними системами на БПЛА забезпечують надійну багатоканальну розвідку, спостереження і рекогносцировку.

Ще одна важлива характеристика – комплексність, тобто поєднання різних засобів РЕР і РЕБ (стаціонарні системи радіоелектронного захисту позицій, районів та базових таборів; мобільні системи захисту колон (броньована/небронбована техніка, позашляховики, тощо); портативні системи захисту піших патрулів, малих розвід груп; спеціальні системи захисту саперів) в єдину мережу, що значно підвищує ефективність системи.

Кожна система має спеціалізоване ПЗ, яке дозволяє відстежувати поточну РО на всіх рівнях управління в режимі онлайн, а система підтримки прийняття рішень забезпечує синхронізоване, узгоджене застосування техніки РЕБ в різних точках базування.

Структурно такі комплекси складаються з наступних систем: розмежування доступу до інформації; обліку та відображення вхідної і вихідної інформації; геоінформаціної системи; обліку об'єктів прикриття; обліку даних про системи звязку та засоби РЕБ своїх військ та противника; обліку радіочастот, на яких заборонено створення завад; обліку норм частотно-територіального рознесення; розрахунку імовірної кількості РЕЗ противника на напрямку; розрахунку електромагнітної сумісності між засобами РЕБ.

Отже, враховуючи світовий досвід та виклики сьогодення, розвиток перспенктивної АСУ військами РЕБ ЗС України має базуватися на принципах: інтегрованості, що передбачає об'єднання усіх наземних та повітряних засобів РЕБ; системності розвитку всіх підсистем і елементів; багатофункціональності та адаптованості до зміни радіоелектронної обстановки; комплексного підходу до автоматизації управління; можливості еволюційної модернізації та нарощування функціональних можливостей.

Виходячи з цих принципів, пріоритетними напрямками розвитку АСУ військами РЕБ є: збалансований і комплексний розвиток засобів РЕБ з урахуванням оптимізації складу і структури військ РЕБ в перспективному вигляді ЗС України; створення принципово нових комплексів РЕБ на базі уніфікованих рухомих одиниць і модульних комплектів програмно-апаратних засобів; вдосконалення інформаційних ресурсів системи управління військами РЕБ; розробка нових методів і засобів збору, обробки, подання, зберігання і використання даних РЕР; забезпечення інформаційної взаємодії при спільному виконанні завдань військами РЕБ ЗС України, іншими військами, військовими формуваннями та органами; розробка систем комп'ютерного моделювання, що дозволять виробляти практичні рекомендації щодо ведення РЕБ у бойових операціях.

Проте, розвиток такої системи може бути сповільнений наступними проблемами: виробнича база більшості комплексів РЕБ залишилась на тимчасово окупованій території Сходу України; відсутність у більшості вітчизняних розробників належного досвіду з розробки складних, багатофункціональних АСУ РЕБ; відсутність взаємодії різноманітних засобів РЕБ; висока вартість обладнання.

Висновки: таким чином, реалізація перелічених напрямів розвитку АСУ РЕБ дозволить привести існуючу організацію управління підрозділами РЕБ у відповідність з вимогами сьогодення і значно (щонайменеше в 2-3 рази) скоротити тривалість циклу централізованого управління військами РЕБ та привести його до масштабу часу, близькому до реального. Це в сукупності має забезпечити підвищення ступеня використання бойових можливостей військ РЕБ в залежності від ланки управління щонайменше в 1,5 – 2 рази.

ЛІТЕРАТУРА

1. Alberts D. S., Garstka J. J., Hayes R. E., Signori D. A. Understanding Information Age Warfare. – Washington: CCRP, 2001. – 319 p. 332.

2. Smith E. A. Effects Based Operations. Applying Network Centric Warfare in Peace, Crisis, and War). – Washington: CCRP, 2006. – 602 p.

3. Dombrowski P. J., Gholz E. Ross A. L. Military Transformation and the Defense Industry After Next: The Defense Inductrial Implications of NetworkCentric Warfare. – Newport: Naval War College, 2002. – 127 p.

4. Чепков І.Б., Нор П.І. Загальні тенденції розвитку озброєння та військової техніки // Озброєння та військова техніка. – 2014. – № 1 (1). – С. 4 – 13.

5. Попов А.О., Ремесло В.Я. Особливості ведення радіоелектронної боротьби в спеціальних операціях // Труди Академії. – 2005. – № 58. – С. 136 – 142.

6. Міроненко П.О., Мельник С.С., Попов А.О., Поривай В.О. Рекомендації щодо підвищення ефективності захисту угруповань військ і об'єктів від ураження системами високоточної зброї в операції ОСШР // Труди Академії. – 2006. – № 70. – С. 18 – 25.

Драглюк О. (ВІТІ)
Шкорупський В. (ВІТІ)
Ревуцький В. (ВІТІ)

ПРОГРАМНИЙ КОМПЛЕКС ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПРИ ПЛАНУВАННІ ЗВ'ЯЗКУ „РЕСУРС-С" МОЖЛИВОСТІ ТА ПОРЯДОК ВИКОРИСТАННЯ

В доповіді розглядаються основні можливості програмного комплексу підтримки прийняття рішень при плануванні зв'язку „Ресурс-С".

1. Планування зв'язку

Метою планування зв'язку є забезпечення максимально ефективного використання бойових спроможностей усіх наявних у розпорядженні відповідного начальника зв'язку сил та засобів у ході виконання завдань зі зв'язку.

Планування бойового застосування військової частини (підрозділу) зв'язку полягає у розробці найбільш ефективних способів застосування сил і засобів зв'язку, які є у підпорядкуванні командира військової частини або підрозділу зв'язку, для виконання визначених старшим штабом завдань зі зв'язку.

Планування у загальному вигляді включає три послідовних та взаємопов'язаних етапи:

організація планування,

вироблення та затвердження замислу,

розроблення плану.

Час, відведений для планування бойового застосування, зазвичай, розподіляється: на перший етап – до 10 % (перша фаза – 2 – 3 %; друга – 7 – 8 %); на другий етап – 30 – 40 % (третя фаза – 20 – 25 %; четверта – 10 – 15 %); на третій етап – 50 – 60 % (п'ята фаза – 40-50%; шоста – до 10 %).

2. Інформаційна і обчислювальна підтримка основних процесів, що реалізовуються при плануванні зв'язку

В рамках Розробки програмних засобів підтримки прийняття рішень з організації зв'язку „Ресурс-С" реалізовані наступні елементи: бази даних (БД) та програмні модулі, які забезпечують взаємодію користувача з БД та автоматизації вирішення інформаційно-розрахункових задач, що необхідні при плануванні зв'язку.

Для забезпечення коректної роботи програмного комплексу ПК повинен задовольняти наступним мінімальним вимогам: 1. Комп'ютер – не нижче *CPU* 2 Ггц, *RAM* 2 Гб, місце на *HDD* не менше 4 Гб. 2. Операційна система – *MS Windows 7* та вище з підтримкою кирилиці.

Програмний комплекс складається з наступних модулів (Рис. 1):

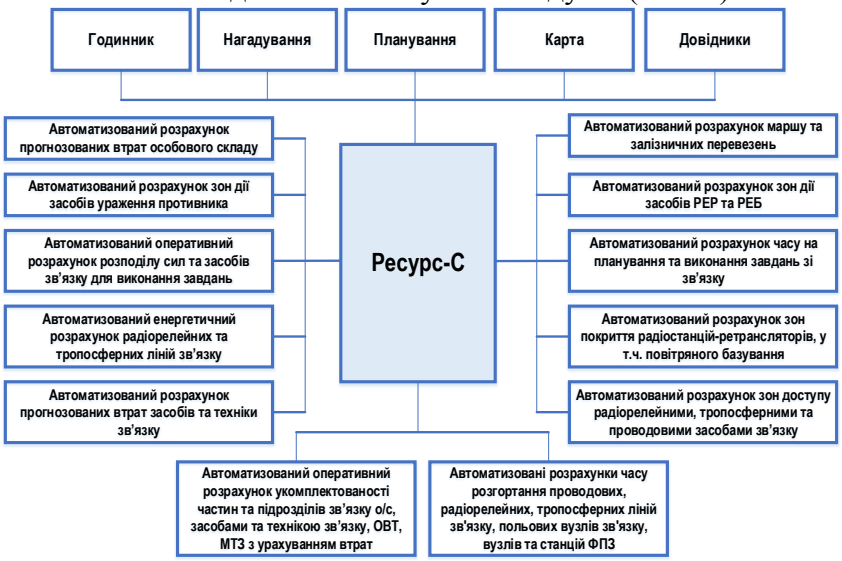


Рис. 1. Загальна структура програмного комплексу „Ресурс-С"

Програмний модуль „Годинник” відображає значення оперативного та астрономічного часу (години, хвилини) і дати (день, місяць, рік) у цифровому форматі.

Програмний модуль „Нагадування” забезпечує введення, коригування та відображення текстових повідомлень і часу нагадування про них. Режим (візуальний, звуковий) та періодичність нагадування (кількість нагадувань, проміжок часу між нагадуваннями, вмикання/вимикання) вводиться (коригується) користувачем для кожного нагадування. Під час процесу нагадування користувач має можливість вимкнути звуковий сигнал окремо та/або вимкнути (закрити) вікно нагадування в цілому (Рис. 3).

Модуль „Планування” забезпечує відображення етапів , фаз і процедур планування зв’язку, а також перехід до планувальних та директивних документів, що відпрацьовуються у ході поточного етапу, фази та процедури, виклику їх програм-редакторів за допомогою ієрархічної системи програмних кнопок виклику відповідних планувальних, директивних та , за потреби, довідкових документів. (Рис. 4).

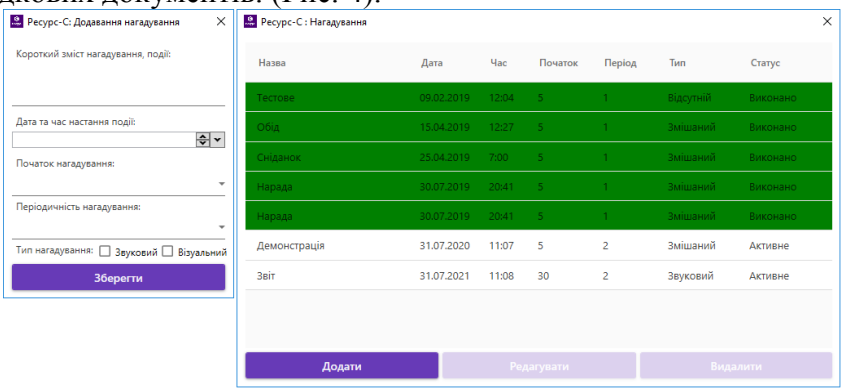


Рис. 3. Вікна модуля „Нагадування”

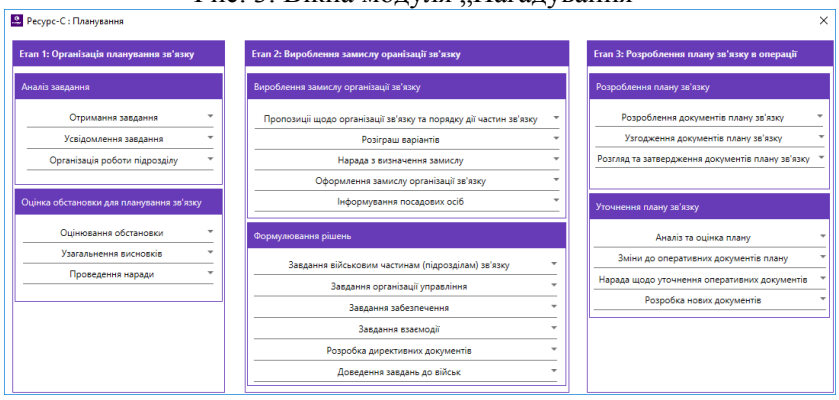


Рис. 4. Вікно модуля „Планування”

Модуль „Довідники” забезпечує виклик на екран та відображення довідкової інформації з БД, її відкриття, створення, коригування, зберігання, тощо (Рис. 5-6).

База даних забезпечує введення, зберігання, пошук та оброблення даних щодо:

наявності засобів ураження, РЕБ та РЕР противника в складі його угруповань;

відомостей про важливі елементи (об’єкти) території, зокрема об’єкти телекомунікацій, доступні пункти відбору телекомунікаційних ресурсів від телекомунікаційної мережі загального користування та телекомунікаційної мережі спеціального призначення (далі - ТМЗК та ТМСП відповідно);

відомостей про елементи системи зв’язку Збройних Сил України;

довідкової інформації.

Програмний модуль „Карта” забезпечує роботу з електронною картою. До даних обстановки належать відомості про рельєф, рослинність та гідрографію території, дорожню мережу, мостові переходи та інші елементи інфраструктури, пункти відбору телекомунікаційних ресурсів від ТМЗК та ТМСП, вежі КРРТ та операторів мобільного зв’язку.

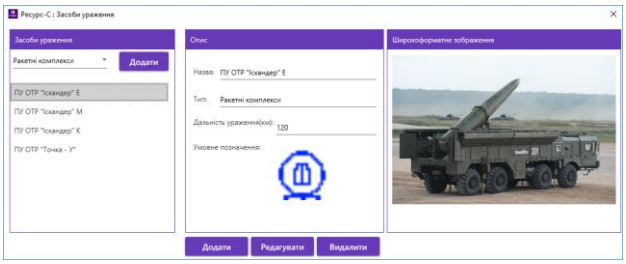


Рис. 5. Довідник „Засоби ураження”

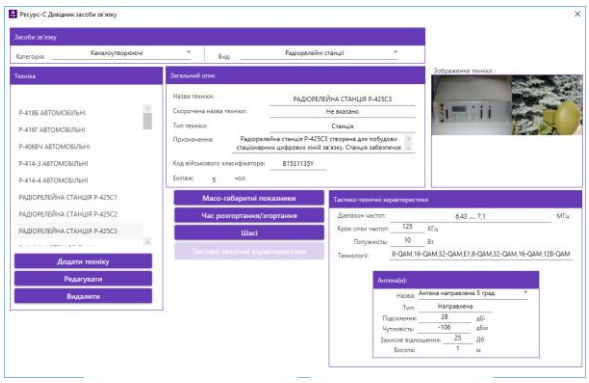


Рис. 6. Довідник „Засоби зв’язку”

Розрахунковий програмний блок “Інформаційно-розрахункові задачі” забезпечує автоматизоване вирішення обчислювальних задач при плануванні зв’язку. До таких задач належать програмні модулі:

а) автоматизований розрахунок часу на планування та виконання завдань зі зв’язку;

б) автоматизований розрахунок зон дії засобів РЕР та РЕБ противника;

в) автоматизований розрахунок зон дії засобів ураження противника;

г) автоматизований розрахунок прогнозованих втрат особового складу;

д) автоматизований розрахунок прогнозованих втрат засобів та техніки зв’язку;

е) автоматизований розрахунок зон доступу радіорелейними, тропосферними та проводовими засобами зв’язку;

є) автоматизований розрахунок зон покриття радіостанцій-ретрансляторів, у т.ч. повітряного базування;

ж) автоматизований енергетичний розрахунок радіорелейних та тропосферних ліній зв'язку;

з) автоматизовані розрахунки часу розгортання проводових, радіорелейних, тропосферних ліній зв'язку, польових вузлів зв’язку, вузлів та станцій ФПЗ;

и) автоматизований розрахунок маршу та залізничних перевезень, та ін.

Програмний модуль „Автоматизований розрахунок часу на планування та виконання завдань зі зв’язку” призначений для створення документу розрахунок часу на проведення планування (Рис. 10).

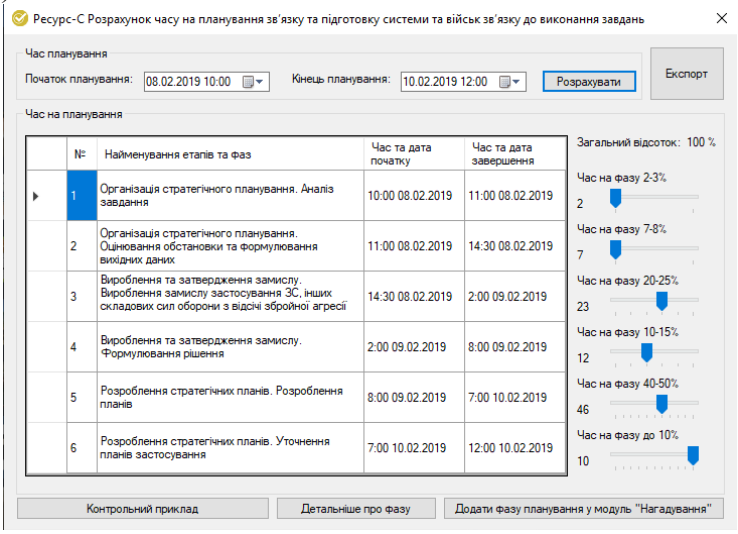


Рис. 10. Модуль „Автоматизований розрахунок часу на планування та виконання завдань зі зв’язку”

Програмні модулі „Автоматизований розрахунок зон дії засобів РЕР та РЕБ противника” та „Автоматизований розрахунок зон дії засобів ураження противника” дозволяють визначати потенційну зону вразливості від засобів РЕБ та РЕР, а також засобів ураження. Тактико-технічні характеристики засобів знаходяться у відповідних довідниках.

Програмні модулі „Автоматизований розрахунок зон доступу радіорелейними, тропосферними та проводовими засобами зв'язку" використовує модуль „Карта" та визначає відповідні зони доступу засобів, відповідно до їх технічних характеристик, що знаходяться у відповідних довідниках (Рис. 11).

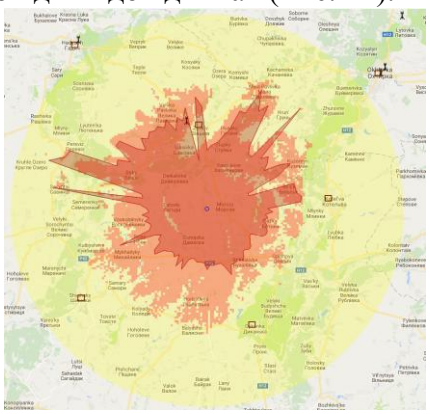


Рисунок 11. Модуль „Автоматизований розрахунок зон доступу радіорелейними, тропосферними та проводовими засобами зв'язку" – результати розрахунку зони дії РРС

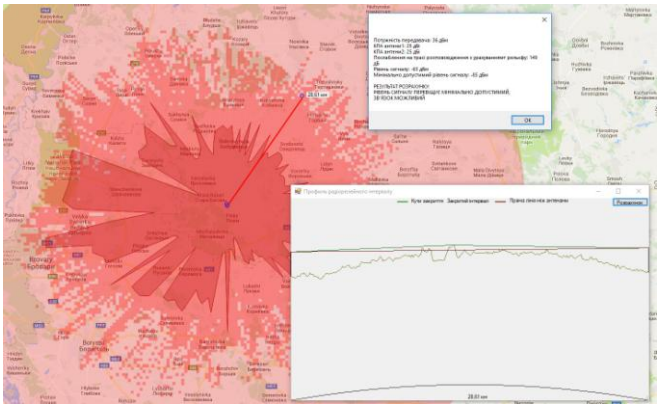


Рисунок 12. Модуль „Автоматизований енергетичний розрахунок радіорелейних та тропосферних ліній зв'язку" – результати розрахунку зони дії РРС

Модуль „Автоматизований енергетичний розрахунок радіорелейних та тропосферних ліній зв'язку" забезпечує розрахунок значень рівня сигналу у точці прийому сигналу з врахування умов рельєфу, технічних характеристик засобів (Рис. 12).

Програмний модуль „Автоматизований розрахунок часу розгортання проводових, радіорелейних, тропосферних ліній зв'язку, польових вузлів зв'язку, вузлів та станцій ФПЗ" дозволяє отримувати значення часу розгортання окремих станцій апаратних, а також вузлів зв'язку, що з них складаються (Рис. 13).

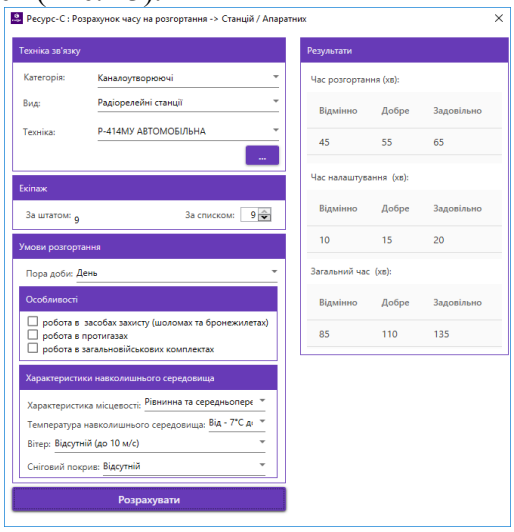


Рис. 13. Модуль „Автоматизований розрахунок часу розгортання станцій/апаратних"

Решта модулів, на даний момент, дозволяють отримувати значення в табличних редакторах та формах.

На даний час, завершилися приймальні випробування, які показали правильність вибраного напрямку досліджень та проведені успішно.

За результатами випробувань було отримано ряд пропозицій, та намічені наступні функції, що потребують автоматизації та які будуть втілені в наступній версії програмного комплексу.

Духанов М.А. (ТОВ „Радіо Сатком Груп”)

НОВІ ТА ПЕРСПЕКТИВНІ ВИДИ РОБОТИ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ТЕХНІКИ ЗВ’ЯЗКУ L3HARRIS

Актуальність. Сучасні цифрові радіостанції L3Harris, все частіше використовуються для роботи у складі систем управління тактичного рівня, в той самий час відбувається збільшення кількості радіостанцій в ЗС України. З огляду на це, основним завданням є інтеграція обладнання зв’язку з різними програмними комплексами, що розробляються для виконання різноманітних завдань. Крім того, L3Harris створює нові форми сигналів, щоб максимально задовольнити вимоги по передачі даних для систем управління, та оптимізує вже існуючі форми сигналів для роботи різних сервісів яким необхідна передача даних. Також виробник постійно удосконалює форми сигналів для ефективної роботи в бойових умовах.

Радіостанції L3Harris виконані як радіопристрій з програмованими параметрами (Software-defined radio – SDR), і для застосування нових форм сигналів у радіостанції, достатньо оновити мікропрограму радіостанції. Таким чином, незмінюючи апаратну частину радіостанції ми збільшуємо її можливості.

Відповідно, важливою є взаємодія розробників програмного забезпечення з представниками виробника для вчасної оптимізації роботи систем управління.

Мета. Ефективне застосування можливостей обладнання зв’язку L3Harris з системами управління тактичного рівня ЗС України.

Основні положення

Знання можливостей програмного забезпечення радіостанцій корпорації L3Harris, як запорука ефективного практичного застосування радіозасобів в усіх ланках управляння ЗСУ. Оновлення мікропрограм змінює на програмному рівні функції (можливості) радіозасобів, Враховуючи значний вплив програмного забезпечення на роботу засобів зв’язку, використання нових мікропрограм радіостанцій та програмних засобів потребує також змін в їх обліку.

Для впровадження цих механізмів важливо наступне:

для мікропрограм та програмних засобів створити окремий облік. Окрім обліку слід створити окреме сховище для мікро програм так сховище для застосунків;

розподілити права та обов’язки щодо оновлення радіостанції серед військовослужбовців ЗС України таким чином, щоб оновленням радіозасобів здійснювалось кваліфікованим персоналом, який пройшов інструктаж (тренінг) в навчально-тренувальному центрі ТОВ „Радіо Сатком Груп”);

налагодити інформування виробників програмного забезпечення про те, які можливості з передачі даних у яких режимах мають радіостанції. Створити рекомендації для виробників програмного забезпечення щодо інтерфейсів та протоколів передачі даних;

створити рекомендації щодо програмування радіостанцій, коли радіостанція використовується у тактичних системах управління або є канало-утворюючою для інших застосунків;

детальне вивчення нових режимів роботи, зі створенням рекомендацій по застосування цих режимів;

огляд нових режимів роботи КХ та УКХ радіостанції.

Висновки

Побудова ефективної системи управління тактичного рівня, як результат спільної роботи фахівців у галузі зв’язку з розробниками систем управління.

Дюков І. М. (ЖВІ)

АЛГОРИТМ ВИЯВЛЕННЯ ТА ФОРМУВАННЯ РАДІОПЕРЕШКОД ЛІНІЯМ РАДІОЗВ'ЯЗКУ З ШИРОКОСМУГОВИМИ СИГНАЛАМИ

Актуальність. Важливе місце в забезпеченні переваги управління військами та зброєю в сучасних бойових діях (операціях) посідає радіоелектронна боротьба. Протягом останніх років спостерігається збільшення невідповідності рівня розвитку радіоелектронних засобів, призначених для управління військовою технікою та засобами, що стоять на озброєнні іноземних держав, можливостям з радіоелектронного виявлення та радіоелектронного подавлення засобів радіоелектронної боротьби Збройних Сил України.

Завданням дослідження є необхідність модернізації або розробки нових засобів радіоелектронної боротьби, які забезпечать задану оперативність та якість радіоелектронного подавлення ліній радіозв’язку противника в ході ведення бойових дій.

Основні положення. Сучасні радіоелектронні засоби, як правило, використовують широкосмугові сигнали (ШСС) для здійснення радіозв’язку. Сьогодні до кінця не вирішеним завданням є виявлення та радіоелектронне подавлення ліній радіозв’язку з ШСС. Традиційні методи модуляції (АМ,ЧМ) були розроблені, в свій час, з урахуванням максимальної концентрації потужності в центрі виділеної смуги частот. Широкосмугові системи спроектовані з метою мінімізації середньої потужності для будь-якої частоти за рахунок розширення спектра сигналу та підвищення надійності передачі даних за рахунок збільшення надмірності інформації. Spread Spectrum (SS) системи використовувалися винятково для військових та наукових цілей. Властивості, що робили ці системи привабливим для військових, роблять їх ідеальними і для цивільного використання. Це стійкість до перешкод і навмисного втручання, труднощі у виявленні і перехопленні, а також можливість закриття інформації. Завдяки розширенню спектра сигналу помітно зменшується вплив електромагнітних перешкод на цілісність сигналу (при тривалому впливі). Завада, що з'являється в смузі частот SS сигналу, може вразити тільки дуже маленьку частину всієї смуги, а тому, що переданий сигнал розподілений на весь спектр, він буде надійно відновлений у приймачі.

ШСС відповідної тривалості можна одержати за допомогою частотної або фазової маніпуляції, де закон маніпуляції може бути обраний за відповідним алгоритмом. Уся сукупність кодових послідовностей, що використовується для формування ШсС, поділяється на два класи: ортогональні (квазіортогональні) і псевдовипадкові (ПВП – послідовності з низьким рівнем взаємної кореляції). У якості модулюючих послідовностей найбільшого поширення набули: М-послідовності [1]; нелінійні М-послідовності [2, 3]; послідовності Голда та Касамі [2, 3]; послідовності Лежандра та Якобі [2, 3]; послідовності Баркера; послідовності Якобі.

Пропонується варіант реалізації алгоритму виявлення та формування радіоперешкод лініям радіозв’язку з ШСС. Це дозволить підвищити ймовірність виявлення ліній радіозв’язку з ШСС, визначення параметрів радіосигналів та формування ефективних радіоперешкод.

Висновки. Наводиться математичне забезпечення алгоритму та сам алгоритм виявлення та формування радіоперешкод лініям радіозв’язку з ШСС. Представлено результати досліджень розробленого алгоритму щодо виявлення ШСС та формування радіоперешкод ЛРЗ з такими сигналами, проведеного методом імітаційного моделювання.

ЛІТЕРАТУРА

1. Шумоподобные сигналы в системах передачи информации. Под ред. В.Б.Пестрякова. – М. Сов.Радио, 1973. – 424 с.

2. Варакин Л.Е. Системы связи с шумоподобними сигналами. М. Радио и связь, 1985. 383 с.

3. Сумик М., Прудіус І., Сумик Р. Теорія сигналів. –Львів. 2005. – 190 с.

д.т.н. Єрохін В.Ф. (ІСЗЗІ „КПІ”)
Ірха М.С. (ІСЗЗІ „КПІ”)

МЕТОДИКА І РЕЗУЛЬТАТИ АНАЛІЗУ ЗАВАДОСТІЙКОСТІ ДЕМОДУЛЯТОРА ФМ-СИГНАЛА З КОМПЕНСАЦІЄЮ ПОДІБНОЇ ПЕРЕРИВЧАСТОЇ ЗАВАДИ

В роботі [1] був виконаний синтез алгоритму розділення корисного і заважаючого сигналів з двійковою фазовою модуляцією, асинхронних за тактовими точками за додаткової умови про переривчастий характер випромінювання завади. На відміну від відомого [2] алгоритму компенсації заважаючого сигналу в [1] вирішена задача синтезу компенсації завади, що характеризується довільним асинхронізмом за тактовими точками відносно корисного сигнала.

Метою доповіді є викладення методики і результатів аналізу завадостійкості алгоритму демодуляції – розділення, одержаного в [1]. Вираз для імовірності помилки в оцінці r_1^{k*} дискретного параметра r_1^k корисного сигнала в загальному випадку за додаткових умов $p(r_1=0)=p(r_1=1)=0,5;\quad p(r_2=0)=p(r_2=1)=p(r_2=2)=1/3,\quad P_в=2/3$ має вигляд:

$$P_{пом}=\frac{1}{2^3 3^2}\sum_{r_1^{k-1}=0}^{1}\sum_{r_1^{k}=0}^{1}\sum_{r_1^{k+1}=0}^{1}\sum_{r_2^{k-1}=0}^{2}\sum_{r_2^{k}=0}^{2} p\left(r_1^{k*}=1-r_1^k / r_1^{k-1}, r_1^k, r_1^{k+1}, r_2^{k-1}, r_2^k\right); \qquad (1)$$

$$r_1=\overline{0,1};\quad r_2=\overline{0,2}.$$

За умови вищезазначеної апріорної рівноімовірності станів ДП $r_1^{k-1}, r_1^k, r_1^{k+1}$ та активних станів ДП r_2^{k-1}, r_2^k необхідно буде обраховувати не $2^3 3^2=72$, а лише 36, умовних за станом ДП r_1, r_2 імовірностей в загальному співвідношенні (1). Це пов’язано з тим, що за вищезазначеної умови справедливою є попарна тотожність умовних імовірностей помилки, наприклад:

$$p(r_1^{k*}=0/r_1^{k-1}=0, r_1^k=1, r_1^{k+1}=0, r_2^{k-1}=0, r_2^k=0)=p(r_1^{k*}=1/r_1^{k-1}=1, r_1^k=0, r_1^{k+1}=1, r_2^{k-1}=1, r_2^k=1), \qquad (2а)$$

або

$$p(r_1^{k*}=0/r_1^{k-1}=1, r_1^k=1, r_1^{k+1}=0, r_2^{k-1}=2, r_2^k=0)=p(r_1^{k*}=1/r_1^{k-1}=0, r_1^k=0, r_1^{k+1}=1, r_2^{k-1}=2, r_2^k=1). \qquad (2б)$$

Тобто, на підставі (2а), (2б) можна стверджувати, що існує 36 пар «антиподів», що можна використати для зменшення трудомісткості обрахування імовірності помилки за формулою (1) вдвічі. Власне, ця формула дещо спроститься:

$$P_{пом}=\frac{1}{2^2 3^2}\sum_{r_1^{k-1}=0}^{1}\sum_{r_1^{k+1}=0}^{1}\sum_{r_2^{k-1}=0}^{2}\sum_{r_2^{k}=0}^{2} p\left(r_1^{k*}=1/r_1^{k-1}, r_1^k=0, r_1^{k+1}, r_2^{k-1}, r_2^k\right). \qquad (3)$$

Після нормування і центрування, вираз для умовної імовірності помилки буде мати вид:

$$p\left(r_1^{k*}=1-r_1^k/r_1^{k-1}, r_1^k, r_1^{k+1}, r_2^{k-1}, r_2^k\right)=\frac{1+(-1)^{r_1^{k*}}}{2}-(-1)^{r_1^{k*}}\times$$
$$\times\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\int_{-\infty}^{(ArthZ_{k-1}+ArthZ_k-m_1)/\sigma_1}\omega(x_1,x_2,x_3,\rho)\,dx_1dx_2dx_3, \qquad (4)$$

де функції $Arth(...)$ містять змінні інтегрування $x_2=\frac{b_{21}-m_{21}}{\sigma_2^2};\quad x_3=\frac{b_{22}-m_{22}}{\sigma_2^2}$. Тобто, виконана підстановка $b_{21}=\sigma_2^2+m_{21};\quad b_{22}=\sigma_2^2+m_{22}$.

Залишилось застосувати вираз (4) для умовної імовірності помилки в загальному співвідношенні для розрахунків безумовної імовірності помилки.

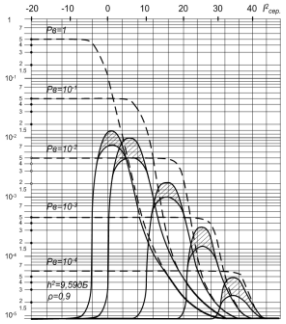


Рис. 1 Імовірність помилки при впливі мерехтливої малоімовірної асинхронної завади

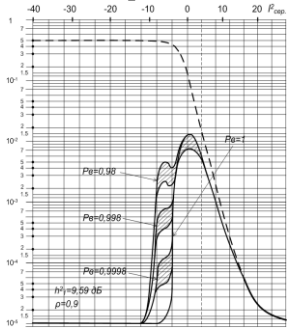


Рис. 2 Імовірність помилки при впливі мерехтливої високоімовірної асинхронної завади

Результати розрахунків потенціальної завадостійкості наведені на рис. 1, 2. Неперервними лініями на всіх графіках представлені залежності імовірності помилки в демодуляції корисного двійкового сигнала від відношення середніх потужностей сигнал/завада $l^2_{сер} = l^2 \times P_в$ при оптимальній компенсації мерехтливої подібної завади у відповідності з алгоритмом [1], пунктирними – при класичному прийомі, коли виявлення і компенсація завади не виконуються. Всі графіки побудовані для нормованого значення коефіцієнта неортогональності $\rho = R / \sqrt{h_1^2 h_2^2} = 0,9$, що відповідає заваді, структура якої досить близька до структури корисного сигнала. Наприклад, для завади і сигнала фазоманіпульованих псевдовипадковими двійковими послідовностями (ПСП), що відрізняються лише структурами ПСП, значення $\rho = 0,9$ еквівалентне неспівпадінням 5 % їх субелементів. Величина $h_1^2 = 9,59\,дБ$ вибрана, виходячи із вимог до імовірності помилки $P^*_{пом} = 10^{-5}$ в каналі без завади.

Висновки. 1. Асинхронізм мерехтливої завади, подібної корисному ЦС, не є підставою для принципової можливості її компенсації. 2. Найгірша завадозахищеність алгоритму компенсації мерехтливої завади спостерігається за умови її синхронізму за тактовими точками і в області, коли завада за миттєвою потужністю не перевищує корисний сигнал більше, ніж на $6\,дБ$ або менша за нього на $8-15\,дБ$. 3. Одержані результати узагальнюють опубліковані раніше в [1 – 3] і підтверджують принципову можливість компенсації завад з переривчастим випромінюванням, подібних до корисного цифрового сигнала.

ЛІТЕРАТУРА

1. Єрохін В.Ф. Методика і результати синтезу компенсатора асинхронної переривчастої завади, подібної до корисного фазоманіпульованого сигнала / Єрохін В.Ф., Ірха М.С. // Сучасні телекомунікаційні системи та захист інформації (Зб. Наукових праць) – : К., 2019, № 1 (5), с. 11 – 22.

2. Бураченко Д.Л. Потенциальная помехоустойчивость демодулятора цифрового сигнала с компенсацией структурной прерывистой помехи / Бураченко Д.Л., Ерохин В.Ф. // Радиотехника. – 1989, № 9, с. 61 – 62 / Деп. в ЦНТИ „Информсвязь”. – 1989, № 1463, с. 34.

к.т.н. Животовський Р. М. (ЦНДІ ОВТ ЗС України)

МЕТОДОЛОГІЧНІ ОСНОВИ УПРАВЛІННЯ РАДІОЧАСТОТНИМ РЕСУРСОМ СИСТЕМ РАДІОЗВ'ЯЗКУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Розвиток інфокомунікаційних технологій, які визначаються зростанням обсягів трафіку і появи нових послуг, призводить до необхідності постійного зростання і модернізації телекомунікаційних систем. Проблемними особливостями надання послуг бездротового зв'язку є: постійне зростання швидкості передачі даних; обмеженість числа частотних каналів; невисока ефективність використання частотного ресурсу, внаслідок статичного розподілу частот за ліцензіями. Тому при експлуатації безпроводових мереж в першу чергу необхідно контролювати завантаженість частотного ресурсу і проводити пошук незайнятих частотних каналів, які тимчасово не використовуються первинними ліцензійними користувачами. У цьому напрямі одним із ключових підходів до підвищення ефективності використання частотного ресурсу є використання методів управління і механізмів, що базуються на принципах когнітивності. Проте, більшість відомих алгоритмів виявлення незайнятих частотних каналів малопридатна для ефективної роботи в задачах радіомоніторингу в когнітивних радіомережах і в даний час розробка алгоритмів визначення незайнятих частотних каналів, орієнтованих на застосування в умовах апріорної невизначеності щодо діючих в робочій смузі сигналів є актуально науково-прикладною задачею.

В ході проведеного в роботі дослідження отримані наступні наукові результати, новизна яких полягає в наступному:

1. Запропоновано нові методи виявлення незайнятих частотних каналів в когнітивних радіомережах, які відрізняються використанням методів виявлення невідомих сигналів на фоні шуму в умовах апріорної невизначеності, які базуються на зміні імовірнісних властивостей спостережень. Запропоновані методи дозволяють підвищити ефективність визначення незайнятих частотних каналів в когнітивних радіомережах.

2. Отримали подальший розвиток методи виявлення невідомих сигналів, що засновані на зміні імовірнісних властивостей спостережень, відмінною особливістю яких є використання інформації тільки про шум у частотному каналі і прийняття рішень у спектральній області.

3. Вперше досліджено робочі характеристики спектральних методів виявлення невідомих сигналів з використанням реальних сигналів і шумів у частотному діапазоні, що використовується для когнітивних радіомереж.

4. Вперше вирішена задача розпізнавання заданих сигналів при наявності невідомих сигналів під час радіомоніторингу в когнітивних радіомережах, відмінною особливістю якої є використання навчальних вибірок тільки для заданих сигналів. Використання запропонованих алгоритмів селекції і розпізнавання дозволяє уникнути помилки розпізнавання, коли невідомий сигнал може бути визначений як один із заданих.

5. Вперше запропоновано алгоритм визначення незайнятих частотних каналів для їх надання вторинним користувачами когнітивних радіомереж з використанням некласичних методів виявлення та розпізнавання сигналів в умовах апріорної невизначеності.

Запропоновані нові спектральні методи виявлення невідомих сигналів на фоні заданого шуму, а також розпізнавання сигналів, заданих навчальними вибірками, при наявності невідомих сигналів. Порівняльний аналіз ефективності алгоритмів виявлення сигналів дозволив дати рекомендації щодо їх практичного використання. При апріорній невизначеності щодо параметрів сигналів первинного користувача рекомендується використовувати алгоритми, які засновані на виявлені зміни статистичних властивостей сигналів. Коли параметри сигналів первинного користувача відомі і є в базі даних, рекомендується використання алгоритмів, заснованих на виявленні властивостей циклостаціонарності або метод узгодженої фільтрації.

к.т.н. Жук О. Г. (ВІТІ)

МЕТОД ФОРМУВАННЯ КАНАЛЬНИХ СИГНАЛІВ В СИСТЕМАХ З OFDM

В сучасних системах радіозв'язку широко використовується один із методів формування широкосмугових сигналів – метод ортогонального частотного розділення з мультиплексуванням (Orthogonal Frequency Division Multiplexing – OFDM). Ідея OFDM полягає в тім, що потік переданих даних розподіляється по множині частотних підканалів і передача ведеться паралельно у всіх цих підканалах. При цьому висока швидкість передачі досягається саме за рахунок одночасної передачі даних по всіх підканалах, а швидкість передачі в окремому підканалі може бути і невисокою. Нова технологія передачі в цей час розглядається як одна з найбільш перспективних для побудови широкосмугових систем цифрового радіозв'язку багатопроменевими каналами, що забезпечує досить високу частотну ефективність цих систем. Основними перевагами даної технології є відносно висока стійкість щодо частотно-селективних завмирань і вузькосмугових завад, а також висока спектральна ефективність.

Разом з тим необхідно відзначити, що в системах з OFDM використовуються сигнально-кодові конструкції у вигляді ортогональних базисів із прямокутною формою імпульсу, частотна характеристика якого описується виразом $sin(x)/x$. Це не дозволяє мінімізувати частотну локалізацію канального сигналу і, таким чином, забезпечити мінімальну чутливість до міжканальної інтерференції. Тому в зазначеній технології, вводять захисні частотні інтервали, у вигляді частотних підканалів, в смузі яких інформація не передається. Введення захисних інтервалів дозволяє зменшити рівень позасмугових випромінювань сигналу і, як наслідок, мінімізувати вплив на суміжні канали інтерференційних завад. Але даний підхід істотно знижує ефективність використання виділеного частотного ресурсу. При цьому величина захисних інтервалів в системах радіозв'язку з OFDM становить близько 25 % від усього виділеного частотного ресурсу.

Запропоновано новий метод формування канальних сигналів для підвищення ефективності використання виділеного частотного ресурсу в системах радіозв'язку з OFDM. Суть методу полягає в тім, що замість базису Фур'є, використовується базис власних векторів субсмугових матриць, вектори якого мають кращу частотно-часову локалізацію, забезпечуючи менший рівень внеполосных випромінювань синтезованого канального сигналу.

У запропонованому методі використовується принцип формування дискретних канальних сигналів, заснований на розв'язанні оптимізаційної задачі по мінімізації просочування енергії сигналу за виділений частотний інтервал.

Як показало комп'ютерне моделювання, сигнали сформовані на основі базису власних векторів субсмугових матриць мають досить низький рівень позасмугових випромінювань. При цьому ступінь локалізації енергії у виділеному частотному інтервалі можна контролювати значеннями власних чисел, вибираючи такі власні вектори, власні числа яких не перевищують заданого значення.

Таким чином, використовуючи властивість мінімізації енергії за виділеним частотним діапазоном у синтезованих канальних сигналах, можна знизити вимоги до величини захисного інтервалу. Це дозволяє формувати канальний сигнал у більш широкій смузі частот (не перевищуючи при цьому границі виділеного частотного ресурсу), що забезпечить передачу більшої кількості інформаційних символів в одному каналі, при мінімальному уровене позасмугових випромінювань.

На підставі цього можна збільшити кількість переданої інформації і, таким чином, підвищити ефективність використання виділеного частотного ресурсу.

д.т.н. Журавський Ю. В. (ЖВІ ім. С.П. Корольова)
к.т.н. Шишацький А. В. (ЦНДІ ОВТ ЗС України)

МЕТОДОЛОГІЧНІ ОСНОВИ ОЦІНЮВАННЯ РАДІОЕЛЕКТРОННОЇ ОБСТАНОВКИ НА ОСНОВІ НЕЧІТКОЇ КЛАСТЕРИЗАЦІЇ ЧАСОВИХ РЯДІВ

Збільшення кількості радіоелектронних засобів противника на фоні обмежень засобів радіоелектронної розвідки (РЕР) та недосконалості відомих методів (методик) оцінювання радіоелектронної обстановки (РЕО) зумовлює необхідність пошуку нових наукових підходів для підвищення ефективності функціонування багатопозиційної системи РЕР та відповідної системи оцінювання РЕО. Підвищення ефективності функціонування системи оцінювання РЕО може бути досягнуте шляхом удосконалення методів оброблення великих об'ємів інформації від елементів багатопозиційної системи РЕР (постів та мобільних груп РЕР).

Одним із напрямків підвищення ефективності оброблення даних є застосування процедури кластеризації. Оброблення великих об'ємів інформації та їх аналіз за допомогою кластеризації дає змогу оцінити особливості відповідних процесів. Багато інформації, що характеризує великі об'єми даних, міститься в часових рядах. Однак, однією з типових проблем оброблення часових рядів є їх нерівномірне квантування та багатовимірність. Кластеризація одновимірних та багатовимірних часових рядів із нерівномірними тактами квантування ускладнена тим, що для кожного з рядів ці такти можуть бути несинхронізовані, тобто нерівномірними та асинхронно квантованими. Таким чином, забезпечення аналізу часових рядів за допомогою кластеризації для системи оцінювання РЕО є важливим та актуальним науково-практичним завданням.

Для виконання зазначеного завдання в ході проведення досліджень було розроблено методологічні основи оцінювання РЕО на основі нечіткої кластеризації часових рядів, а також відповідні методи нечіткої кластеризації даних РЕО, що послідовно надходять з нерівномірними тактами квантування, на основі апарату гібридних систем обчислювального інтелекту.

Наукова новизна результатів дослідження полягає в такому:

вперше розроблено метод нечіткої кластеризації, який використовує цільову функцію нечіткої кластеризації, що дозволяє вирішувати задачу кластеризації в режимі реального часу за умов перетину класів та асинхронних нерівномірно квантованих часових рядів, а також зменшувати ефект концентрації норм;

вперше розроблено метод послідовної кластеризації багатовимірних часових рядів у режимі реального часу, який базується на апараті гібридних систем обчислювального інтелекту, що дозволяє розв'язувати задачу кластеризації первинних даних РЕО, які послідовно надходять на оброблення з нерівномірними тактами квантування;

отримав подальшого розвитку метод адаптивної кластеризації, який відрізняється використанням імовірнісної та можливісної кластеризації коротких часових рядів, що дозволяє розв'язувати задачу кластеризації нерівномірно квантованих часових рядів, а також спростити чисельну реалізацію методу за рахунок використання метрики на основі тангенсів кутів нахилу;

отримав подальшого розвитку метод робастної адаптивної ідентифікації нестаціонарних часових рядів у режимі реального часу, який відрізняється використанням введеної модифікації критерію Гемана-МакКлюра, що дозволяє розв'язувати задачу оброблення первинних даних РЕО, які збурені аномальними викидами;

вперше запропоновано методологічні основи оцінювання РЕО на основі нечіткої кластеризації часових рядів, які ґрунтуються на вказаних вище методах.

Практичне значення отриманих результатів полягає в тому, що використання запропонованих методологічних основ дозволяє підвищувати ефективність системи оцінювання РЕО при розв'язанні задач кластеризації даних, які послідовно надходять на оброблення з нерівномірними тактами квантування.

Зав’ялов М.О. (ВІТІ)
Гріньков В.О. (ВІТІ)

ОРГАНІЗАЦІЯ МЕРЕЖЕВОЇ РОЗВІДКИ ЗАСОБАМИ ІНТЕРНЕТ СЕРВІСІВ

Вивчення противника з метою виявлення його можливостей і намірів є однією з найстаріших форм інформаційної діяльності. З вдосконаленням формування інформаційного суспільства характер цієї діяльності істотно змінився. З одного боку, з’явилися нові засоби добування та обробки інформації, в тому числі інфокомунікаційні засоби та інформаційні технології, з іншого боку різко зріс обсяг інформації, яку необхідно обробити для отримання необхідних даних про противника. Крім того, різко ускладнилася конкурентна боротьба. Вона набула глобального характеру, стала більш динамічною і менш прогнозованою. У цих умовах потрібні нові підходи до застосування методів та засобів розвідки у кібернетичному просторі, які дають можливість планувати проведення наступальних кібернетичних операцій з метою домінування у кібернетичному просторі над противником та заздалегідь з’ясувати та запобігти спрямованому кібернетичному впливу на критично-важливі об’єкти інформаційно-телекомунікаційних мереж. Тому, підвищення ефективності заходів розвідки у кібернетичному просторі противника є актуальним питанням дослідження.

Аналіз останніх досліджень та публікацій. Незважаючи на безліч проведених досліджень M. S. Dahiya, Howard Chivers, Monowar H. Bhuyan стосовно удосконалення методів кібернетичної розвідки, на наш час ефективного вирішення цієї проблеми немає. Тому вони потребують додаткового і більш глибокого вивчення та аналізу переваг та недоліків пасивного та активного методу кібернетичної розвідки інформаційно-телекомунікаційних мереж противника та визначення шляхів комплексного використання переваг кожного методу при розробці та впроваджені засобу добування розвідувальних даних інформаційно-телекомунікаційних мереж, що підвищить ефективність проведення кібернетичної розвідки в умовах обмеження часу.

Головним фактором, який впливає на процес реалізації кібернетичних атак, є засоби і методи розвідки у кібернетичному просторі, які дають можливість планувати проведення наступальних кібероперацій з метою домінування у кіберпросторі над противником та заздалегідь з’ясувати і запобігти спрямованому кібернетичного впливу на критично-важливі об’єкти інформаційно-телекомунікаційних мереж. Добування інформації може бути використаний для побудови моделі атакуючої системи та полегшення в майбутньому спроби проникнення до неї для реалізації кібернетичного впливу.

Для вирішення даної задачі в контексті мережевої розвідки є доцільним використання інструментів віддаленого аналізу та ідентифікації досліджуваних об’єктів противника такі як: *Strobe, Tcp_scan, Udp_scan, Nmap, Netcat, SuperScan, IpEye, WUPS, Fscan*. Проте, незважаючи на той факт, що нині питанню побудови інструментів добування розвідувальних даних приділена велика увага, головним питанням залишається – ефективне застосування інструментів розвідки кіберпростору.

Отже, за аналізом досліджень можливо дійти висновку, що найбільш сприятливим засобом кібернетичної розвідки є Nmap, який дає змогу на достатньому рівні провести розвідувальні заходи, щодо дослідження віддаленого об’єкта противника. Водночас, враховуючи переваги зазначеного засобу добування розвідувальних даних над іншими, слід відмітити, що в умовах обмеження часу цей інструмент віддаленої ідентифікації досліджуваного об’єкта не здатний у короткі проміжки часу добути бажану розвідувальну інформацію про противника. Тому це обумовлює актуальність подальших досліджень, які полягають у розробленні та впровадженні розподіленої системи кібернетичної розвідки досліджуваного об’єкта противника, що дасть можливість скоротити використання часу на виконання добування розвідувальної інформації у ході проведення розвідувальних заходів.

к.т.н. Зайцев О.В. (ВДА ім. Євгенія Березняка)

МЕТОДИЧНИЙ ПІДХІД ДО ВИЗНАЧЕННЯ ПЕРЕВАГ ГІПОТЕЗ, ПРЕДСТАВЛЕНИХ У ВИГЛЯДІ КОНКУРУЮЧИХ ІНТЕРВАЛЬНИХ ОЦІНОК

Актуальність. В процесі розробки та вдосконалення сучасних інформаційних систем підтримки прийняття рішень спеціального призначення (СППР) виникають наступні проблеми: не завжди можна отримати весь необхідний обсяг апріорної інформації (має місце так звана епістемічна невизначеність – epistemic uncertainty), а з іншого боку, як мінімум частина даних, які використовуються, чутливі до непередбачуваних змін у часі (еліторна невизначеність – aleatory uncertainty). Перебуваючи в частково невизначеній ситуації, експертній підсистемі досить важко давати однозначні і жорсткі оцінки досліджуваних об'єктів і процесів. Більш адекватними виглядають так звані м'які оцінки (soft estimates), одним з різновидів яких є інтервальні оцінки.

Постановка задачі. Завдання визначення переваг тієї чи іншої гіпотези при комплексуванні експертних оцінок в інтервальному вигляді, при тому що діапазони значень ймовірностей прямої і протилежної гіпотези можуть перетинатися унеможливлює застосування традиційних методів теорії ймовірності. Тому **метою** дослідження є розроблення методичного підходу до комплексування інформації у вигляді конкуруючих інтервальних оцінок з метою визначення переваг тієї чи іншої гіпотези в СППР.

Основні положення. Припустимо, експертна система (експерти) мають оцінити стан певного об'єкту. Для вирішення цієї задачі кожний експерт може застосувати інтервальний підхід та сформувати індивідуальну м'яку (soft estimate) оцінку ймовірності такої події у вигляді інтервального числа [1]. Нехай для оцінки стану об'єкту залучено групу експертів, при цьому за результатами вивчення наявної інформації частина експертів дійшла висновку про наявність загрозливого стану об'єкту, а друга частина експертів – висновку про відсутність загрози. Завдання полягає в тому, щоб визначити, якій із висновків експертів є найбільш ймовірним. Для вирішення цього завдання обчислимо відстані між інтервальними числами, які відповідають оцікам [2], за виразами відстані Хаусдорфа-Чавента (Hausdorff-Chavent distance), Евклідової відстані (Euclidean distance), відстані Вассерштейна (Wasserstein distance). Далі пропонується провести розрахунки в два етапи. На першому етапі виконується роздільне агрегування сукупностей висновків (оцінок), сформованих експертами зі складу першої і другої підгруп [1]. На другому етапі порівнюються отримані агреговані оцінки і визначається ступінь переваги [2]. Для агрегування оцінок може бути використаний один з відомих методів оптимізації. Отримані агреговані оцінки порівнюються і визначається оптимальна. Формулу для розрахунку ступеня переваги однієї з оцінок над другою оцінкою наведено в [3]. Всі необхідні розрахунки можливо провести в програмному середовищі MathCad з використанням алгоритму пошуку мінімуму функції KNITRO.

Висновок. Розроблений методичний підхід визначення переваг гіпотез дозволяє обробляти діапазони значень ймовірностей суперечливих гіпотез у разі їх часткового перетинання та вирішувати складні завдання в СППР та в подальшому може бути реалізований у вигляді програмного забезпечення.

ЛІТЕРАТУРА

1. Alefeld G., Herzberger J. Introduction to Interval_Computations / NY: Academic Press, 2012. – 352 p.

2. Tran L., Duckstein L. Comparison of fuzzy numbers using a fuzzy distance measure, Fuzzy Sets and Systems, 2002. 130. P. 331–341.

3. Dammak F., Baccour L., Alimi A.M. An Exhaustive Study of Possibility Measures of Interval-Valued Intuitionistic Fuzzy Sets and Application to Multicriteria Decision Making. Advances in Fuzzy Systems Hindawi Publishing Corporation. Vol. 2016. Article ID 9185706. URL: http://dx.doi.org/10.1155/2016/9185706

Залевський В. Й. (ЖВІ)

ЗАКРИТТЯ ТЕЛЕКОМУНІКАЦІЙНИХ КАНАЛІВ ЗВ'ЯЗКУ З БЕЗПІЛОТНИМ ЛІТАЛЬНИМ АПАРАТОМ

Безпілотні літальні апарати (БПЛА) на сьогодні довели свою здатність високоефективно вирішити військові завдання – проведення тактичної розвідки, враження цілей боєприпасами, управління коригуванням вогню під час бойових дій та ураженні поодиноких цілей.

У даний час існує низка технічних проблем, що стримують розвиток БПЛА і їх застосування, у тому числі в зоні проведення Операції об'єднаних сил (ООС), а саме – завантаженість і забезпечення передачі інформації по каналах зв'язку між БПЛА і наземним пунктом управління (НПУ) в необхідному обсязі, із заданою швидкістю і без спотворень.

Якщо перша проблема може бути вирішена шляхом конструктивних змін всього планера і його силової установки, то друга тільки збільшенням пропускної спроможності і завадостійкості каналів передачі інформації.

У доповіді наголошується, що проблему уразливості каналів передачі даних від БПЛА каналами зв'язку на даному етапі більш доцільно вирішувати за допомогою закриття лінії зв'язку криптографічними засобами, а також домагатись автономності БПЛА при використанні противником засобів радіоелектронної боротьби.

Починаючи з 2014 року увага до захисту каналів передачі даних тільки зростає і з оцінки дій в зоні проведення ООС випадків перехвату управління БПЛА майже нема.

Вимоги, що пред'являються до каналів зв'язку в цілому, включають засоби для закриття інформації, які представлені на ринку у широких межах.

При оцінюванні вимог, які висуваються до системи захисту каналу зв'язку (СЗКС) криптографічними методами, можна виділити такі аспекти як: швидкодія, надійність шифрування, масогабаритні показники бортовий частини СЗКС. Дані фактори вступають в протиріччя між собою, особливо при підвищених вимогах до пропускної спроможності каналу і невеликій масі БПЛА.

Найбільш поширеними в світі криптографічними алгоритмами і протоколами які застосовуються є RSA, DSA, KCDSA, ECDSA, EC KCDSA, EC-GDSA. Тому при створенні і модернізації БПЛА потрібно визначити вимоги і до систем передачі даних.

На вибір алгоритму шифрування впливає ряд факторів, як організаційних (зокрема, питання сертифікації), так і технічних, серед яких важливим моментом є реалізація на наявній елементній базі. Конфігурація та оптимізація алгоритмів які застосовують при створювані системи захисту каналу зв'язку, дозволяють забезпечити захищений канал зв'язку так і самої інформації.

Автором було проаналізовано і змодельовані системи з симетричним блоковим шифром AES і новими методичними рекомендаціями стандарту шифрування ДСТУ 7624:2014 року для найбільш поширених комунікаційних інтерфейсів RS-232 та типу USB. ДСТУ 7624:2014 визначає десять різних режимів роботи (застосування), які широко поширені відповідно до міжнародного стандарту SO/IEC 10116:2006. Наявність такої кількості режимів роботи надає можливість ефективної реалізації систем, засобів і протоколів криптографічного захисту інформації в інформаційно-телекомунікаційних системах передачі даних так і збереженню інформації.

Підвищена увага до інформаційної безпеки, зокрема, закриття телекомунікаційних каналів зв'язку з БПЛА дозволить захистити найбільш критичні дані (канали управління, розвіддані) шляхом залучення БПЛА на тактичному полі бою під час активного проведення радіоелектронної боротьби противником.

Зарубенко А.О. (ВІТІ)
Палівода В.С. (ВІТІ)
Мартинюк А.В. (ВІТІ)

СТАН ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ЗАСОБІВ РАДІОЗВ'ЯЗКУ В ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Радіозв'язок є невід'ємною частиною системи зв'язку (СЗ), як складової системи управління військами. Як свідчить досвід, провідних країн світу, системи управління розвиваються в напрямі створення мультисервісної системи, яка інтегрує функції управління військами, зброєю і зв'язком. Виклики сьогодення вимагають впровадження та використання сучасних засобів зв'язку, в свою чергу, буде неможливо максимально розкрити їх потенціал без зміни ставлення до управління частинами та підрозділами. В середині 2014 року підрозділи ЗСУ та НГУ почали широкого використовувати радіозасоби (РЗ) транкінгового зв'язку компанії „Motorola". Ефективність застосування цих РЗ пов'язана, з невеликими габаритами і стійкістю до перешкод, а технологія TDMA – забезпечила високу ефективність використання радіочастотного ресурсу шляхом створення двох логічних каналів в межах одного фізичного. Крім того, функції дистанційного управління РЗ (блокування, передача GPS координат, програмування), використання алгоритмів шифрування (базовий або AES), можливість інтеграції в мережу на базі IP протоколів (IP site connect) – змінила існуюче на той час уявлення про радіозв'язок.

З початку 2015 року, в зоні проведення АТО, противник почав широко застосовувати комплекси радіоелектронної боротьби. Це призвело до необхідності технічного вдосконалення СЗ ЗСУ. У зв'язку з цим, на озброєння ЗСУ були прийняті РЗ виробництва Harris, Aselsan, Elbit. Нові технічні рішення, впроваджені в РЗ зазначених виробників, дозволили отримати нові можливості, як від СЗ так і від системи управління в цілому. До переваг використання цих радіостанцій можна віднести: забезпечення надійної роботи у радіомережі в різних режимах роботи (телефонний та передача даних). Радіостанції мають новітню систему шифрування, захист від радіоелектронних засобів боротьби противника – режим псевдовипадкової перебудови робочої частоти. Окремо слід виділити можливість автоматичної ретрансляції та маршрутизації інформації (MANET).

Вийти на новий технічний рівень засобам радіозв'язку дозволило застосування SDR (Software-Defined Radio) технології. Принцип SDR – об'єднання можливостей комп'ютера і радіостанції. Радіостанції, які використовують SDR мають можливість автоматично змінювати параметри радіочастоти, виконувати адаптацію до спектру перешкод, протоколів, працювати як ретранслятор. Найбільша перевага SDR – отримання користувачем мультисервісних послуг в одному пристрої. Якщо порівняти показники якості зазначених РЗ (надійності, взаємосумісность), то перевага належить радіостанціям КХ-діапазону – Harris. По-перше, вони забезпечують надійне шифрування трафіку всієї мережі за допомогою алгоритмів AES або Citadel. По-друге, це можливість отримання мультисервісних послуг в режимі роботи MTNW (самоорганізованих та децентралізованих радіомереж).

Порівнюючи РЗ УКХ-діапазону, за своїми можливостями, слід відмітити РЗ Aselsan, які найкраще відповідають вимогам сухопутних, морських і військово-повітряних сил (створює можливість встановлювати на різні зразки озброєння). Крім того, вони адаптовані до спільної роботи з радіостанціями „Motorola", які є найпоширеніші в ЗСУ.

Наступним кроком після SDR може бути створення РЗ з інтелектуальним керуванням, які автоматично зможуть встановлювати зв'язок в реальному часі. Підхід до побудови інтелектуальних радіосистем, що отримав назву когнітивне радіо (CR – когнітивне радіо, IEEE 802.22), є передовою технологією. Технологія дозволяє системі отримувати знання про середовище експлуатації, про діючі правила і про свій внутрішній стан; динамічно і автономно коригувати свої експлуатаційні параметри і протоколи згідно отриманих знань для досягнення заздалегідь поставлених цілей і вчитися на основі отриманих результатів.

к.т.н. Здоренко Ю.М. (ВІТІ)
Кузнєцов Д.Р. (ВІТІ)

МЕТОДИ ОБРОБКИ ВЕЛИКИХ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ВІЙСЬКОВО-МЕДИЧНИХ ЗАКЛАДІВ

Автоматизація обробки даних в інформаційних системах військово-медичних закладів є невід'ємною складовою розвитку медичної галузі.

Вона дозволяє збільшити продуктивність обробки даних та спростити документообіг у військово-медичних закладах. Зростання обсягів інформації, які зберігаються в інформаційних системах визначає вимоги до механізмів їх якісної обробки. Такі механізми повинні забезпечувати відповідність часових показників з виконання запитів на пошук необхідної інформації та надавати можливість виявляти неявні залежності в даних. В сучасних інформаційних системах існує ряд невирішених задач, пов'язаних з накопиченням великої кількості інформації та необхідністю її обробки для подальшого аналізу.

Так, в накопичених даних можуть міститися неявні причинно-наслідкові зв'язки, що можуть бути використані для підтримки прийняття управлінських рішень. Накопичені дані можуть мати різний ступінь структурованості, що впливає на кінцеві показники оцінки якості їх обробки. Тому актуальною є задача розробки відповідних механізмів аналізу великих даних в таких інформаційних системах.

Об'єктом дослідження є процес обробки великих об'ємів даних в інформаційних системах військово-медичного закладу.

Предметом дослідження є методи обробки великих об'ємів даних, які використовуються для автоматизації процесів документообігу в військово-медичному закладі.

Метою роботи є покращення показників якості процесу аналізу великих об'ємів даних шляхом розробки та впровадження нових методів їх обробки в інформаційних системах військово-медичних закладів.

Керівництво військово-медичного закладу має потребу в періодичній систематизації та узагальненні накопичених даних за визначений проміжок часу.

Така інформація необхідна в процесі прийняття управлінських рішень.

Більшість існуючих механізмів аналізу даних в військово-медичних інформаційних системах здійснюють їх аналітичну обробку на основі традиційних підходів, що ґрунтуються на статистичних методах. Використання інформаційних систем з розподіленою архітектурою дозволяє здійснювати накопичення та обробку даних на множині вузлів мережі.

Така архітектура визначає вимоги до механізмів обробки таких даних. Одним з найпоширеніших підходів пошуку неявних закономірностей в даних є застосування методів інтелектуального аналізу даних (Data Mining). Застосування методів Data Mining дає можливість розв'язати наступні задачі: класифікації (Classification); кластеризації (Clustering); асоціації(Associations); прогнозування (Forecasting); візуалізації (Visualization) та інші. Розподілена архітектура інформаційної системи передбачає використання розподілених механізмів обробки даних, замість зберігання даних в одній файловій системі, дані зберігають та індексують на множині вузлів.

Також створюється карта (map), в якій міститься інформація про місцезнаходження тих чи інших даних. Прикладами таких систем, є системи на основі фреймворків Hadoop та Apache Spark.

Тому аналітичну обробку даних для розподілених військово-медичних інформаційних систем пропонується здійснювати на основі інтеграції методів Data Mining з механізмами розподіленої обробки даних.

Для цього в подальшому пропонується розробити програмний модуль аналітичної обробки, що дозволить виявляти неявні закономірності в великих обсягах даних.

к.т.н. Здоренко Ю.М. (ВІТІ)
к.т.н. Лаврут О.О. (НАСВ)
Диган Д.І. (ВІТІ)

МЕТОД АНАЛІТИЧНОЇ ОБРОБКИ ДАНИХ ПРО ПАРАМЕТРИ ТРАФІКУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

На сьогоднішній день аналіз мережевого трафіка є актуальною задачею. Стрімкий розвиток мережевої галузі, а саме впровадження нових мережевих протоколів прикладного рівня вимагає вирішення завдань забезпечення інформаційної безпеки в інформаційно-телекомунікаційних мережах загального та спеціального призначення. Тому актуальною є задача знаходження неявних ознак, які притаманні аномальному трафіку. Одним з шляхів вирішення цієї задачі є застосування сніферів для захоплення трафіка з його подальшим аналізом. Аналіз трафіка, що пройшов через сніфер, дозволяє: виявити паразитний, вірусний і закільцьований трафік, наявність якого збільшує завантаження мережного устаткування і каналів зв'язку; виявити в мережі шкідливе і несанкціоноване програмне забезпечення, наприклад, мережеві сканери, троянські програми; перехопити будь-який незашифрований (а деколи і зашифрований) призначений для користувача трафік з метою отримання даних ідентифікації та іншої інформації.

Метою роботи є підвищення ефективності процесу аналізу мережевого трафіка в мережах загального та спеціального призначення на основі інтелектуальних методів.

Об'єктом роботи є процес аналізу мережевого трафіка.

Більшість сучасних сніферів зберігають дані про захоплені пакети в спеціальному файлі з форматом *pcap* (*Packet Capture*). Аналіз даних в файлах в режимі реального часу за таких умов стає не можливим. При роботі множини таких моніторів трафіку, які можуть знаходитись в різних місцях мережі, одночасний доступ до такого файлу для запису та читання даних є неможливим. Тому є необхідність в розробці нових підходів, які дозволять усунути зазначений недолік.

Вищезазначені фактори визначають потребу в пошуку нових рішень для архітектури систем захоплення трафіка та нових методів його аналізу. Так, виходячи з специфіки задачі пропонується розподілена архітектура системи моніторингу. Така архітектура передбачає розміщення сніферів в множині вузлів мережі для захоплення трафіка та передачі даних моніторингу в єдиний вузол обробки. Результати захоплення трафіка з множини вузлів мережі передаються до вузла з загальною базою даних, де в подальшому пропонується здійснювати їх аналітичну обробку. Тому основними етапами методу аналітичної обробки даних параметрів трафіка комп'ютерної мережі пропонується обрати наступні: попередній збір та передавання параметрів трафіку в єдину базу даних; формування аналітичних вибірок для отриманих даних на основі обробки наданих з використанням засобів системи керування базою даних; додаткова аналітична обробка даних моніторингу; видача даних за результатами аналізу та їх візуальне представлення. Додаткову аналітичну обробку пропонується здійснювати на основі інтелектуальних методів аналізу. Для цього пропонується розробити програмний модуль аналітичної обробки даних моніторингу на основі цих методів.

Проведений аналіз показав, що підхід побудови систем моніторингу трафіка з розподіленою архітектурою має значні переваги в порівнянні з локально розміщеними сніферами. Розгортання такої розподіленої системи потребує додаткових рішень аналітичної обробки та узагальнення даних. В подальшому планується розробити програмний модуль аналітичної обробки даних моніторингу, що дозволить виявляти аномальний трафік та знаходити причини його виникнення.

Зроль С.С. (ВІТІ)
Троцько О.О. (ВІТІ)

АНАЛІЗ БЕЗПЕЧНОГО МЕРЕЖЕВОГО ДОСТУПУ НА БАЗІ ПЛАТФОРМИ CISCO ISE

На сьогоднішній день в Збройних силах України (ЗСУ) постає питання інформаційної захищеності. Велика кількість небезпек що загрожує країні може мати як зовнішнє так і внутрішнє походження. Багато випадків втрати даних в мережах особливо при використанні не захищеного доступу до корпоративних мереж. Для ЗСУ є важливим розробити платформу для контролю доступу до мереж спеціального призначення та захистити їх від зовнішніх атак. Платформа яка може забезпечити захищеність інформації, конфіденційність обміну інформацією та безперервності управління військами та озброєнням є Cisco Identity Services Engine (ISE). Реалізація платформи Cisco ISE є рішення для контролю доступу до корпоративної мережі з урахуванням контексту доступу. Рішення об'єднує сервіси автентифікації, авторизації та обліку подій (AAA), оцінки стану, профілювання і управління гостьовим доступом в рамках єдиної платформи. Cisco ISE автоматично виявляє і класифікує кінцеві пристрої, забезпечує необхідний рівень доступу, проводячи автентифікацію як користувачів, так і пристроїв, а також забезпечує відповідність кінцевих пристроїв корпоративній політиці інформаційної безпеки (ІБ) шляхом оцінки їх стану захищеності перед наданням доступу до корпоративної ІТ-інфраструктури. Платформа підтримує гнучкі механізми контролю доступу, включаючи групи безпеки, мітки груп безпеки і списки контролю доступу груп безпеки. Сьогодні зазначені вище пріоритети є дуже важливими для збереження інформації що циркулює в мережах передачі даних, а також повного контролю мережі з відстеженням користувачів та можливістю обліку їх дій.

Основними особливостями платформи Cisco ISE є:

– Проведення автентифікації корпоративних користувачів і кінцевих пристроїв – надання можливості визначити яким корпоративним користувачам та пристроям дозволено отримати доступ до мережі.

– Забезпечення авторизації корпоративних користувачів і кінцевих пристроїв – визначає до яких мережевих ресурсів дозволений доступ користувачеві та пристрою, які успішно пройшли автентифікацію.

– Використання корпоративними користувачами особистих пристроїв, що дозволяє користувачеві реєструвати особисті пристрої, з яких буде дозволений обмежений доступ до мережі.

– Надання AAA для мережевого обладнання – забезпечення єдиного місця автентифікації, авторизації та обліку доступу адміністраторів до мережного обладнання, без необхідності створення багатьох локальних облікових записів і правил доступу на цих пристроях.

Платформа Cisco ISE є дуже високо затратною в підтриманні її повного функціоналу. Але на сьогоднішній день існує багато безкоштовних програм та додатків. Додаток Kismet, який дозволяє всебічно аналізувати мережевий трафік та виявляти в ньому аномалії. Також NeDi, програмне забезпечення, яке сканує мережу по MAC-адресам, IP-адресам і DNS та встановлює з них власну базу даних. За допомогою цих безкоштовних програм та додатків можливе створення єдиної платформи для контролю доступу до корпоративної мережі з урахуванням контексту доступу. На сьогоднішній день для ЗСУ є дуже важливим використання платформ та додатків для інформаційної захищеності та збереження даних в мережах спеціального призначення. Тому, створення аналогу платформи Cisco ISE з інформаційної безпеки в ЗСУ є головним питанням на сьогоднішній день. Дана платформа з контролем доступа є ефективним методом для забезпечення повного контролю мережі та захисту особистих даних в мережах спеціального призначення. Використання аналогу Cisco ISE забезпечить зручне управляння мережею, повного контролю корпоративних користувачів та контролю над межевими атаками з зовні та середини мережі.

Івченко М.М. (НЦЗІ ВІТІ)
Ткач В.О. (НЦЗІ ВІТІ)
Мусієнко В.А. (НЦЗІ ВІТІ)
Шугалій О.О. (НЦЗІ ВІТІ)
Очіченко Р.А. (НЦЗІ ВІТІ)

АНАЛІЗ ІСНУЮЧИХ ПРОБЛЕМ ЩОДО ЗАБЕЗПЕЧЕННЯ ЗІП СУЧАСНИХ ЗАСОБІВ ЗВ'ЯЗКУ ТА АВТОМАТИЗАЦІЇ

В Збройних силах України у зв'язку з реформуванням органів управління технічним забезпеченням військ зв'язку, перерозподілом їх функцій та повноважень, існує певна проблема щодо збору корректної інформації з відмов сучасних засобів зв'язку та автоматизації, її обробки, узагальнення, визначення якісних та кількісних показників певних видів відмов, яка вкрай необхідна для відповідних розрахунків різних видів ЗІП до сучасної техніки зв'язку. Зазначене може призвести в подальшому до недостатньої або навпаки надмірної (завищеної) кількості комплектуючих елементів, які повинні входити до складу ЗІП, що в подальшому не дозволить повноцінно обслуговувати та ремонтувати пристрої та засоби зв'язку на місці їх експлуатації (при недостатній кількості елементів ЗІП), чи призвести до перевитрати ресурсів на надлишкові елементи ЗІП.

Аналіз отриманих з військ даних щодо відмов сучасної техніки зв'язку під час ведення бойових дій показав, що більшість відмов склалася внаслідок експлуатації поставлених зразків з відхиленням від інструкцій з експлуатації та відсутності будь-яких видів ЗІП до них взагалі. Також, в наданих даних відсутня будь-яка статистика щодо виходу з ладу елементів від часу їх напрацювання на відмову, а інформація щодо кількісних та якісних показників, стосовно поставлених в Збройні сили України зразків сучасної техніки зв'язку, недостатня для проведення будь-яких розрахунків щодо кількості та комплектності відповідних видів ЗІП на сучасну техніку.

В той же час, обґрунтований склад та кількість ЗІП може надати лише організація-розробник (виробник) на основі аналізу напрацювання на відмову та наявності відомостей стосовно показників надійності складових частин виробу, отриманих при відповідних випробуваннях та випробуваннях дослідних зразків, експлуатації виробів-аналогів, а також встановлених показників надійності в нормативно-технічній документації на складові частини виробу та його особливостей функціонування, видів розподілення часу безвідмовної роботи виробів (складових частин) і часу їх відновлення та термінів служби всіх комплектуючих елементів виробу в порівнянні з загальним терміном служби всього виробу.

Склад комплектів відповідних видів ЗІП до новітньої техніки зв'язку повинен визначатися відповідно до вимог ГОСТ В 15.501–90.

Слід зазначити, що за розробку видів ЗІП, їх комплектність, кількість, якість та норми їх витрат згідно вимог ГОСТ В 15.705 відповідає тільки головний розробник (розробник), при чому методику розрахунку складу комплектів ЗІП розробник повинен узгоджувати з замовником.

Види комплектів ЗІП (одиночний ЗІП-О, груповий ЗІП-Г та ремонтний ЗІП-Р) для визначеного виробу повинні задаватися замовником в ТТЗ (ТЗ) на виконання ДКР.

Номенклатура та кількість запасних частин, що входять до складу комплектів ЗІП-О, ЗІП-Г повинні розраховуватися з урахуванням забезпечення заданих в ТТЗ (ТЗ) на виконання ДКР вимог щодо надійності виробів (п.3.1.1 ГОСТ В 15.705).

На вимогу замовника, яка вказана в ТТЗ (ТЗ) на виконання ДКР для окремих видів виробів розробник (виробник) виробу повинен розробляти, виготовляти та постачати комплекти ЗІП, враховуючи специфічні особливості експлуатації та їх обслуговування (п.2.1 ГОСТ В 15.705). При чому номенклатуру та якісний склад комплектів ЗІП-О та ЗІП-Г розробник повинен встановити (розрахувати) по узгодженню з замовником при розробці виробів, а для комплектів ЗІП-Р – при розробці ремонтної документації (п.2.2 ГОСТ В 15.705).

На вироби, до яких розраховується комплект ЗІП-О, розробник по узгодженню з замовником (в ТТЗ (ТЗ) на виконання ДКР) обов'язково встановлює напрацювання на відмову чи термін служби виробу, а для розрахунку ЗІП-Г в ТТЗ (ТЗ) додатково встановлюють кількість виробів (п.2.6.2, п.2.7.2 ГОСТ В 15.705)

Кількість виробів, на які розробляють комплект ЗІП-Р встановлює замовник в ТТЗ (ТЗ) на розробку ремонтної документації в залежності від виду, методів, об'єму ремонту та розміру серії виробів, що виготовляються (п.2.8.2 ГОСТ В 15.705).

З початку 2014 року в Збройних силах України лише нижчепойменовані зразки озброєння та військової техніки, були прийняті на озброєння в результаті проведення дослідно-конструкторських робіт (далі – ДКР) на замовлення Міністерства оборони України відповідно до вимог чинного законодавства, а саме, радіорелейні станції Р-425С1, Р-425С2, Р-425С3, Р-414МУ авто., Р-414МУ-01 авто., Р-414МУ-02 авто., Р-414МУ-03 авто, вироби В271-Л, О171, О171-01.

Усі інші системи, комплекси, засоби зв'язку та автоматизації були прийняті на озброєння в результаті проведення ініціативних ДКР, визначальних відомчих випробувань або матеріальної допомоги іноземних країн, внаслідок чого всі майнові та немайнові права на поставлені в Збройні сили України засоби по сьогодняшній день належать їх виробникам. Таким чином, представники Міністерства оборони України жодним чином не можуть впливати на зміст технічної документації та склад комплектів поставки, також відсутня можливість внесення жодних змін в тактико-технічні завдання на ДКР щодо розробки зазначених зразків внаслідок їх відсутності або їх закриття, внаслідок чого подальша робота щодо отримання даних виходу з ладу зразків ОВТ та їх складових з метою визначення складу ЗІП є недоцільною.

Єдиним шляхом виходу зі складеної ситуації вбачається проведення переговорної процедури щодо внесення змін в правочини (договори), що укладені між Міністерством оборони України та виробниками (розробниками) щодо визначення обґрунтованого складу та кількості ЗІП до зразків з врахуванням вищезазначених до них вимог відповідно до чинного законодавства.

ВИСНОВОК

1. Вирішення визначеної проблеми можливе тільки шляхом внесення змін в договори, що укладені між Міністерством оборони України та виробниками (розробниками) в частині, що стосується розробки видів ЗІП, їх комплектності, кількості, якісних характеристик та норм витрат ЗІП на кожний виріб з врахуванням обґрунтованих пропозицій з військ, які повинні базуватися на статистиці щодо виходу з ладу елементів від часу їх напрацювання на відмову

2. По кожному виробу безпосередньо з розробником (виробником) на основі наданого ним повного комплекту документації на виріб включаючи робочу конструкторську документацію, комплекти документації на всі складові елементи виробу, комплекти документації з відомостями при покупці елементів виробу, (відповідно до ГОСТ В 15.705 та ГОСТ В 15.501-90) доцільно провести дослідження з визначенням обґрунтованого складу та кількісті ЗІП з врахуванням показників надійності кожного з елементів виробів.

ЛІТЕРАТУРА

1. Донесення командирів військових частин зв'язку на ГУЗІС ГШ Збройних сил України щодо відмов сучасних засобів зв'язку та автоматизації та потреби ЗІП в період 2014-2018 роки.
2. Державний стандарт ГОСТ В 15.501-90.
3. Державний стандарт ГОСТ В 15.705-86.
4. Техническая эксплуатация и надёжность средств связи. Издание-Ленинград 1970г.
5. Справочник. Надёжность технических систем. Под редакцией профессора И.А. Ушакова. Глава14. – Обеспечение технических объектов запасными элементами. Автор А.Э. Шура – Бура.

к.т.н. Іщенко Д. А. (ЖВІ)
к.т.н. Кирилюк В. А. (ЖВІ)

МОДЕЛЬ ДЕЗОРГАНІЗАЦІЇ УПРАВЛІННЯ ВІЙСЬКАМИ (СИЛАМИ) ЗА ПРОГНОЗОВАНИМИ ВАРІАНТАМИ КОМПЛЕКСНОГО ЗАСТОСУВАННЯ ПРОТИВНИКОМ ЗАСОБІВ ВОГНЕВОГО УРАЖЕННЯ ТА РАДІОЕЛЕКТРОННИХ ПЕРЕШКОД

Аналіз досвіду проведення антитерористичної операції та операції Об'єднаних сил для забезпечення національної безпеки й оборони, відсічі і стримування збройної агресії Російської Федерації у Донецькій та Луганській областях свідчить про пріоритетність виконання завдань з дезорганізації управління противника у ході проведення операцій (бойових дій).

Важливою умовою забезпечення ефективності дій з досягнення дезорганізації управління військами (силами) виступає комплексне застосування засобів вогневого ураження та радіоелектронного подавлення для приведення в непрацездатний стан радіоелектронних засобів – елементів системи управління.

Потенціальні можливості противника щодо дезорганізації управління військами (силами) підтверджує наявність у нього новітніх засобів ураження, радіоелектронного подавлення та досвід їх достатньо ефективного застосування на території Донецької та Луганської областей.

Можливість комплексного застосування засобів вогневого ураження та радіоперешкод по радіоелектронних засобах, що узгоджено функціонують у складі системи управління відповідно до загального алгоритму управління діями військ (сил), зумовлюють потребу забезпечення стійкого управління військами (силами) в усіх видах дій за рахунок підвищення результативності радіоелектронного захисту радіоелектронних засобів як елементів системи управління. Комплексне застосування противником засобів вогневого ураження та радіоелектронного подавлення для дезорганізації управління військами (силами) потребує своєчасного вирішення завдання вдосконалення науково-методичного забезпечення радіоелектронного захисту радіоелектронних засобів – елементів системи управління.

Відсутність у науково-методичному апараті елементу моделювання прогнозованого комплексного застосування засобів вогневого ураження та радіоелектронного подавлення обмежує можливості з оцінювання дезорганізації управління, що може виникнути за їх результатами, та визначення достатніх заходів для підтримання управління військовими частинами (підрозділами). Тому розроблення моделі дезорганізації управління військами (силами) за прогнозованими варіантами комплексного застосування противником засобів вогневого ураження та радіоелектронних перешкод як складової відповідного науково-методичного апарату є важливим та актуальним науково-практичним завданням.

При розробленні моделі вдосконалено науково-методичний апарат прогнозування та планування радіоелектронного захисту радіоелектронних об'єктів та засобів, які є елементами системи управління підрозділів, частин та угруповань військ (сил).

В умовах сучасних бойових дій за великої кількості радіоелектронних об'єктів і засобів у складі систем озброєння та військової техніки, оцінювання можливостей противника з дезорганізації управління військами (силами) необхідно здійснювати у ході підготовки до бойового застосування. Визначення очікуваного ступеня дезорганізації управління може здійснюватись заздалегідь для фіксованих варіантів вогневого ураження та радіоелектронного подавлення елементів системи управління у визначеному її кількісному та якісному складі, просторовому розташуванні.

Наведено порядок побудови аналітичної моделі вогневого ураження та радіоелектронного подавлення елементів системи управління військами (силами). Аналітичне моделювання здійснюється за рахунок використання адекватних математичних залежностей ступеня дезорганізації управління військами (силами) від можливостей

противника з вогневого ураження та радіоелектронного подавлення радіоелектронних об’єктів та засобів, що є елементами системи управління.

У моделі прийнято, що метою застосування противником засобів вогневого ураження та радіоперешкод є приведення у непрацездатний стан радіоелектронних засобів системи управління військами (силами). Аналітичну модель подано системою співвідношень між заданими характеристиками варіантів застосування противником засобів вогневого ураження та радіоперешкод по радіоелектронних об’єктах та засобах системи управління угруповання військ (сил), у визначених варіантах її побудови, та ступенем дезорганізації, що є шуканою величиною.

Основними способами комплексного вогневого ураження та радіоелектронного подавлення, що прийняті для моделювання: спосіб послідовного застосування наявних призначених противником вогневих засобів та засобів радіоперешкод; спосіб одночасного застосування наявних призначених засобів впливу по елементах системи управління військами (силами). Розроблено варіанти застосування противником засобів радіоперешкод та вогневого ураження, що відрізняються один від одного за кількісними та якісними показниками сукупностей засобів впливу противника і радіоелектронних засобів системи управління, а також їх взаємного розташування у просторі.

Розроблені варіанти дозволяють враховувати черговість застосування засобів вогневого ураження та радіоелектронного подавлення, ефективність радіоелектронного захисту за кількісним показником. Запропоновано математичний апарат, який дозволяє формалізувати вогневе ураження радіоелектронних засобів, що подані моделями одиночного та групового об’єктів. Отримано аналітичні вирази для оцінювання ймовірностей ураження об’єктів для параметрів, що визначають просторове положення елементарних об’єктів, закон розподілу точки падіння засобу ураження, його характеристики. Розроблено модель ураження одиночного (елементарного) та групового військового об’єкта. Модель враховує: склад групового об’єкта, його розміри, розміри елементарних об’єктів; закон розподілу точки падіння засобу ураження за площею; наявність критичних елементарних об’єктів; характеристики засобів вогневого ураження.

Моделі застосування противником засобів радіоелектронного подавлення подано аналітичними виразами, які враховують їх можливості (в першу чергу за енергетичним потенціалом та пропускною здатністю). Пропускна здатність оцінюється для кожного класу радіоелектронних засобів та засобів радіоелектронного подавлення противника шляхом розрахунку відповідних коефіцієнтів охоплення.

Ступені дезорганізації управління визначаються збитком системи управління, який розраховується як частка радіоелектронних засобів, що втрачають працездатність, від загальної кількості їх чисельності, що розраховуються за математичними формулами в явному вигляді.

Отже, розроблена модель дезорганізації управління військами (силами) за прогнозованими варіантами комплексного застосування противником засобів вогневого ураження та радіоелектронних перешкод дозволяє формалізувати процеси оцінювання радіоелектронного захисту радіоелектронних об’єктів та засобів, які є елементами системи управління підрозділів, частин та угруповань військ (сил) для різних умов обстановки. Модель є базою для створення відповідних алгоритмів, які забезпечуватимуть підвищення ступеня автоматизації роботи органів управління в інтересах зростання оперативності прийняття рішень щодо розподілу наявного ресурсу сил і засобів.

Напрямами подальшої роботи з вдосконалення формалізації варіантів радіоелектронного захисту є розроблення програмного забезпечення оцінювання захищеності радіоелектронних об’єктів та засобів, які є елементами системи управління.

Камак Д.О. (ДНДІВС ОВТ)
Руденко О.В. (ДНДІ ВС ОВТ)
Скиба О.В. (ДНДІ ВС ОВТ)
Доманов І.О. (ДНДІ ВС ОВТ)

ПРОБЛЕМИ В РОЗРОБЛЕННІ СУЧАСНИХ АПАРАТНИХ ЗВ'ЯЗКУ

Актуальність доповіді полягає у висвітленні існуючих проблем, які виникли під час розроблення нових зразків техніки зв'язку, а саме: у недотриманні встановленого законодавством України порядку розроблення сучасних апаратних зв'язку; наслідків, до яких це призвело, та у необхідності врегулювання зазначеного питання.

Метою доповіді визначена необхідність висвітлити існуючі проблеми у розробленні сучасних апаратних зв'язку та запропонувати шляхи її вирішення.

З початком російської агресії проти України у 2014 році, у зв'язку з неможливістю використання техніки зв'язку радянського виробництва, яка перебувала на озброєнні агресора, та не забезпечувала належного рівня управління військами, постало питання необхідності забезпечення Збройних Сил України сучасними засобами зв'язку.

З метою розроблення сучасних апаратних зв'язку державним замовником приймались управлінські рішення щодо закладання до апаратних зв'язку радянського виробництва цифрових засобів передачі та обробки інформації з одночасним вилученням аналогового обладнання, що не задовольняло сучасним вимогам.

Найменування апаратних не змінювалось, хоча за результатами переобладнання, фактично, були розроблені нові зразки техніки зв'язку з іншими тактико-технічними характеристики і можливостями. Для розроблених апаратних зв'язку не відпрацьовані: технічні умови, конструкторська, експлуатаційна і ремонтна документація.

Як наслідок, внаслідок порушення порядку розроблення, неможливо провести кодифікацію, введення до штатів і табелів до них та видачу наказу про прийняття на озброєння (постачання) розроблених зразків техніки зв'язку.

Відсутність конструкторської документації (технічних умов), експлуатаційної та ремонтної документації робить неможливим організацію належної штатної експлуатації розроблених апаратних зв'язку, яка є стадією життєвого циклу засобів зв'язку і автоматизації з моменту приймання їх військовою частиною від установи – виробника чи ремонтної установи до списання і є сукупністю наступних етапів: приймання, введення в експлуатацію, приведення в установлену ступінь готовності до використання за призначенням, підтримання в установленому ступені готовності до використання за призначенням, використання за призначенням, зберігання, транспортування, зняття з експлуатації, списання.

Разом з тим, постановою Кабінету Міністрів України від 20.02.2013 № 120 „Про затвердження Порядку розроблення, освоєння та випуску нових видів продукції оборонного призначення, а також припинення випуску існуючих видів такої продукції", передбачений порядок розроблення нових зразків озброєння та військової техніки шляхом проведення дослідно-конструкторських робіт відповідно до оперативно-тактичних (тактико-технічних, загальних) вимог замовника.

Авторами доповіді пропонується привести процес розроблення апаратних зв'язку у відповідність до вимог чинного законодавства, для чого провести наступні заходи: державному замовнику розробити оперативно-тактичні (тактико-технічні, загальні) вимоги до апаратних зв'язку, потреба в яких існує в Збройних Силах України; обґрунтувати доцільність проведення розроблення апаратних зв'язку, фінансову і технічну спроможності їх виготовлення на вітчизняних підприємствах; ініціювати прийняття рішення Кабінетом Міністрів України про розроблення апаратних зв'язку; організувати та провести дослідно-конструкторські роботи щодо створення сучасних апаратних зв'язку; провести кодифікацію і прийняти створені апаратні зв'язку на озброєння Збройних сил України згідно з вимогами діючого законодавства.

Камак Д.О. (ДНДІ ВС ОВТ)
Руденко О.В. (ДНДІ ВС ОВТ)
Скиба О.В. (ДНДІ ВС ОВТ)
Троцик С.М. (ДНДІ ВС ОВТ)

ЗАСТОСУВАННЯ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ЗАСОБІВ ДЛЯ ПІДТРИМКИ АНТИТЕРОРИСТИЧНИХ ДІЙ НА ВІЙСЬКОВИХ ОБ'ЄКТАХ

Актуальність

Загроза нападу на військові об'єкти, особливо місця зберігання зброї та боєприпасів, з боку ворожих диверсантів, терористів або злочинців постійно зростає. Про це свідчать регулярні диверсії, що здійснюються останні роки на арсеналах та базах Збройних сил України, періодичні напади на військовослужбовців, що несуть службу зі зброєю.

Як зазначає досвід проведення силової фази антитерористичних дій (АТД) в різних країнах світу, підрозділи спеціального призначення нерідко несуть втрати, гинуть заручники.

Однією з вагомих причин цього є недостатня обізнаність про ситуацію, яка склалася (характеристика району АТД, кількість терористів, їх розташування, наявне у них озброєння, місця утримання та кількість заручників тощо).

Це й обумовлює актуальність вибору теми доповіді.

Мета. Метою доповіді є висвітлення загальних поглядів щодо можливості впровадження новітніх безпроводових технологій передачі даних в інтересах успішного проведення АТД.

Основні положення. Не дивлячись на те, що АТД можуть проводитися на невеликій за розміром ділянці місцевості або споруді, для її успішності доцільно використовувати спеціальні технічні засоби для збору, обробки та обміну інформацією, функціонально інтегровані в єдину інформаційну систему.

Зазначена система повністю побудована на бездротовій технології передачі інформації. Принцип її функціонування подібний до бездротових сенсорних мереж, які, за потреби, можуть стати складовою (або основою) для побудови системи забезпечення проведення АТД. У зазначеній системі виділяється декілька суб'єктів та об'єктів (або їх груп), що здійснюють інформаційну діяльність (добування та обмін інформацією, її обробку та передачу сигналів (команд, розпоряджень, вказівок) в інтересах АТД:

– органи управління АТД;

– підрозділи (окремі військовослужбовці), що безпосередньо проводять силову фазу АТД або особи, що проводять переговорний процес;

– спеціальні технічні засоби, що залучаються для проведення АТД: портативні радіостанції, сенсорні вузли, наземні роботизовані комплекси, безпілотні літальні апарати, ретранслятори, точки радіодоступу, модулі безпроводового доступу (для під'єдання до ПЕОМ), відоекамери (комбат-камери та WEB-камери), базові станції (за необхідності).

За основним призначенням спеціальні технічні засоби можна поділити на засоби для:

– обміну голосовими повідомленнями;

– добування, попереднього аналізу та передачі обробленої інформації;

– передачі відеоданих, координат та іншої спеціальної інформації;

1. Органи управління АТД.

У них повинна концентруватися більшість інформації, що стосується прийняття рішень для проведення АТД і розвитку ситуації на етапі їх підготовки та під час проведення. Тому технічні засоби, що використовуються ними, повинні бути скомутованими швидкісними каналами з іншими технічними пристроями, що залучаються до АТД:

наземні роботизовані комплекси – для отримання відеоданих та іншої інформації про порушників, заручників, виявлені міни, вибухові пристрої, зброю та іншої інформації;

сенсорні вузли – для моніторингу навколишньої обстановки, її попереднього аналізу та передачі даних про виявлення та характер дій як терористів, так і спецпризначенців, радіаційної, хімічної та іншої обстановки;

безпілотні літальні апарати – для отримання відеоданих та координат;

комбат-камери, якими обладнане спорядження спецпризначенців, – для передачі в режимі реального часу інформації з місць безпосереднього проведення силової фази АТД;

WEB-камери, які встановлені всередині чи ззовні будівель, споруд, транспортних засобів тощо – для передачі відеозображення про район проведення АТД та зміни обстановки в режимі реального часу;

засоби голосового зв'язку – для обміну інформацією з іншими суб'єктами АТД;

базові станції – для забезпечення радіопокриття в районі проведення АТД.

2. Особовий склад спецпідрозділу.

Знаходячись у безпосередній близькості до порушників, саме спецпризначенці миттєво візуально сприймають та оцінюють зміни ситуації в місці їхнього перебування та характер дій злочинців. Вони мають не тільки відповідно реагувати, а й, за можливості, оперативно сповіщати за допомогою голосового зв'язку орган управління. Крім того, комбат-камери, зафіксовані на спорядженні спецпризначенців або вбудовані в спецзасоби (наприклад, у броньований щит, що утримується спецпризначенцем, який перший заходить у приміщення при штурмі), автоматично передають відеоінформацію до органу управління.

В свою чергу, підрозділ спецпризначення може отримувати інформацію безпосередньо від сенсорних вузлів і роботизованих комплексів, що діють поблизу. Це дозволить їм відстежувати та аналізувати рівень небезпек, та враховувати додаткові сприятливі/ несприятливі чинники. В разі наявності резервного спецпідрозділу, ці дані в режимі реального часу передаються йому на планшет чи монітор. Також цьому підрозділу доцільно мати можливість прослуховування голосового обміну між органом управління та основним спецпідрозділом.

3. Особи, що проводять переговорний процес, крім афішованого засобу зв'язку з органом управління АТД, обов'язково повинні бути обладнані наступними прихованим засобами передачі інформації: мікрофон (за допомогою якого орган управління АТД буде освідомлений ходом переговорів або, при захопленні особи, що вела переговори, мікрофон стане прихованим передатчиком голосової інформації), мікровідеокамера, пристрій визначення та передачі координат (на випадок захоплення терористами).

4. Спеціальні технічні засоби розглядаються як пристрої для збору, фіксації, попередньої обробки й передачі інформації. Окремі з них можуть бути частково автономними.

Крім безпілотних літальних апаратів та WEB-камер, в залежності від умов проведення АТД, можуть залучатися роботизовані системи, сенсорні вузли, що спеціалізуються на:

добуванні, розпізнаванні інформації про наявність та кількість людей, транспортних засобів на певній території, їх переміщення (напрям, швидкість);

пошуку та виявленні зброї, мін, вибухівок з проведенням попередньої оцінки та ідентифікації виявлених об'єктів;

оцінці термічної, радіаційної, хімічної та бактеріологічної обстановки у районі АТД.

Для вирішення цих завдань роботизовані засоби обладнуються: спеціальними датчиками та приладами передачі даних, а також можуть програмуватися на виконання певних завдань (маршрут переміщення, якість зображення, періодичність надання інформації), аналіз та розпізнавання добутої (виявленої) інформації, автономність дій.

Сенсорні вузли за допомогою вбудованих датчиків контролю, моніторять та аналізують навколишнє середовище, передаючи результати до органів управління АТД та спецпідрозділу.

Висновок. Використання новітніх безпроводових технологій передачі даних в інтересах проведення АТД сприятиме поінформованості сил та засобів, які її проводять, що дозволить знизити ризик втрат серед своїх підрозділів та загибелі заручників, своєчасно та ефективно застосувати резервні сили та засоби і в цілому забезпечить успішність АТД.

Карасенко І.О. (ВІТІ)

ІНТЕГРАЦІЙНА ПЛАТФОРМА ДЕЛЬТА – НОВИЙ ВИД ЗБОРУ ІНФОРМАЦІЇ

„**Дельта**” – це єдина інтеграційна платформа (ІП) збору інформації про позиції сил противника Збройних сил України, розроблена Центром впровадження та супроводження автоматизованих систем оперативного (бойового) управління Збройних сил України. Метою створення системи „Дельта” є забезпечення командира інформацією про оперативну обстановку для підвищення продуктивності (швидкості та якості) процесу прийняття рішень з управління військами (силами), озброєнням та військовою технікою.

До складу ІП „Дельта” входять наступні підсистеми (модулі), які є її невід’ємними частинами:

1. „**Ядро**” (серверна логіка та база даних) – являє собою WEB-сервер, який реалізує протокол стандартизованого обміну даними ADEM (*Alternative Development and Exchange Method*).
2. „**Дельта Монітор**” – підсистема ІП „Дельта”, що відповідає за відображення та внесення інформації про позиції сил противника з ядра чи в ядро системи „Дельта”.
3. „**Дельта ГІС**” – являє собою сервер, на якому розміщується картографічна інформація в цифровому вигляді, необхідний для забезпечення функціонування модуля „Дельта Монітор”.
4. „**Дельта Чат**” – це сервер, який організовує обмін повідомленнями за протоколом XMPP (*Extensible Messaging and Presence Protocol*).
5. „**Дельта Аналітика**” – це WEB-додаток, який дозволяє здійснювати первинний статистичний аналіз загальної оперативної обстановки.

Інформація про бойову обстановку для прийняття управлінських рішень готується штабом у вигляді паперових карт з різними символами, які відображають розташування дружніх та ворожих військ та іншу важливу інформацію про поле бою. Звичайно, підготовка таких карт займає багато часу, не кажучи вже про те, що відображення в такий спосіб бойової обстановки в динаміці взагалі неможливе.

Однак, розвиток інформаційних систем і технологій та їх впровадження у військову сферу призвели до того, що на сьогодні в розвинених у воєнному відношенні країнах світу підготовка карт з бойовою обстановкою відбувається в електронному вигляді із залученням відповідних підрозділів. Підхід з використанням *Common Operational Picture* (COP - „загальна оперативна картина”), крім звичного планування, забезпечує ефективне та динамічне використання всіх наявних інформаційних ресурсів щодо бойової обстановки. При цьому термін „загальний” (*Common*) означає, що він застосовується до всіх учасників, від найвищого командира до солдата, який безпосередньо зв’язаний з тим чи іншим засобом бойового ураження. „Оперативний” (*Operational*) відноситься до фактичного, переважно представленого „в режимі реального часу» статусу подій та їх розвитку (який рідко відповідає завчасно створеному плану), а також стосується оперативного рівня планування, який відображає множину подій тактичного масштабу, та не відноситься до більш високого, стратегічного рівня. „Картина” означає єдине, комбіноване, графічне, візуальне зображення навколишнього середовища, сил та дій. В сумі застосування COP дає можливість як рядовому солдату, так і найвищому командиру самостійно і негайно розпочати взаємодію щодо досягнення заздалегідь визначених цілей та планів командувачів.

Таким чином, інтеграційна платформа „Дельта” надає можливість командиру швидко і точно наносити достовірну і адекватну інформацію про бойову обстановку, відомості про противника, його позиції, сили та засоби військ, а також відомості про свої сили, позиції та засоби військ.

Кізло Л.М. (НАСВ)
Радзіковський С.А. (НАСВ)
Жук О.В. (НАСВ)

СУЧАСНІ НАПРЯМИ ВДОСКОНАЛЕННЯ ПРОЦЕСУ ПІДГОТОВКИ ВІЙСЬКОВИХ ФАХІВЦІВ

Система військової освіти – основне джерело комплектування Збройних сил та інших військових формувань і правоохоронних органів висококваліфікованими офіцерськими кадрами. Військова освіта, в першу чергу, тактичного рівня в усіх провідних країнах світу – це корпоративна система підготовки військових фахівців, призначення яких – виконувати завдання, які зумовлені специфікою функціонування збройних сил і потребою їх застосування в конкретних умовах. Тому, на сучасному етапі розвитку Збройних сил України особливої актуальності набуває питання удосконалення системи підготовки військових кадрів, з використанням сучасних інноваційних технологій та пошуку оптимальних параметрів організації цього процесу.

Актуальність і гострота питання зрозумілі – розвиток світової цивілізації та освітніх систем призвели до глобалізації всіх процесів в суспільстві і спричинили його перехід від індустріалізації до інформатизації. Ці інновації відбулися в усіх сферах людської діяльності, що вимагає появи інтелектуально та професійно підготовлених фахівців для будь-якої галузі, в тому числі – військової.

З метою визначення ефективності впровадження інноваційних перетворень в систему підготовки сучасних військових кадрів були досліджені деякі аспекти організації та змісту (супроводження) процесу підготовки курсантів Національної академії сухопутних військ (НАСВ) – майбутніх офіцерів ЗС України.

Цей процес передбачає набуття і підтримання на належному рівні не тільки військово-прикладних навиків, але і формування у майбутніх офіцерів професійних знань й умінь, на основі розвитку пізнавальної, інформаційної і комунікативної компетентності. На цьому поприщі особливо істотні зміни спостерігаються в супроводженні навчального процесу курсантів вищого військового навчального закладу (ВВНЗ).

Зміна засобів і технології їх навчання відбувається через впровадження інноваційних компонентів, які спрямовуються, перш за все, на ефективне вирішення завдань підготовки сучасного воїна-професіонала, а також на створення необхідних умов і можливостей для їх подальшої самореалізації.

Новітні розробки і прилади суттєво змінили суспільство і дозволили оптимізувати процес підготовки фахівців. Для цього використовується весь арсенал сучасних технологій, а також планшетні ПК, які розповсюджені в багатьох сферах людської діяльності. Планшетні ПК успішно застосовують в медицині, навчальній і дослідницькій діяльності, в роботі, в проектуванні і моделюванні, чи просто для розваг. Вони ідеально підходять для запису лекцій, розкладів занять, завдяки доступу до Інтернет ресурсу – вивчення електронних підручників, посібників, проведення практичних та дослідницьких робіт, спілкування (обмін інформацією), проведення відеоконференцій, а також використання геоінформаційних систем.

Подібні пристрої вже не поступаються звичним для нас персональним комп’ютерам, дозволяють використовувати надзвичайно реалістичне віртуальне зображення для відпрацювання багатьох елементів ведення бойових дій з використанням сучасної техніки і озброєння, що суттєво оновлює процес підготовки сучасного воїна-професіонала, та мають значні переваги в зручності використання при їх малих габаритах і розмірах. До того ж планшетні ПК використовують різні операційні системи, від популярних Android і Windows, до Unix систем, за допомогою яких можна розробляти програмне забезпечення з елементами імітаційного моделювання.

Під час міжнародних навчань „Rapid Trident-2019”, які, частково, проводилися на Яворівському полігоні, також активно використовувалися сучасні засоби і технології організації навчання підрозділів.

Так під час виконання першої фази командно-штабних навчань застосовувалася система імітаційного моделювання JCATS – це інтерактивний засіб моделювання, який дозволяє імітувати дії за участю багатьох сторін як засіб для проведення об’єднаних навчань, аналізу, досліджень, планування та розіграшу поставлених завдань. В ході другої фази навчань, під час виконання підрозділами бойових дій, підрозділи використовували систему MILES (призначена для імітації умов реального бою з тактичної підготовки і дозволяє імітувати пряме збройне зіткнення підрозділів, у тому числі – з використанням бойової техніки), артилерійські підрозділи використовували планшети для корегування вогню, були задіяні безпілотні літальні апарати (БПЛА) – для ведення спостереження за діями підрозділів під час виконання завдань за призначенням.

Також, при проведенні занять с курсантами НАСВ активно використовується система імітаційного моделювання JCATS – це інтерактивний засіб моделювання, який дозволяє імітувати: операції багатонаціональних сил; операції з підтримки миру; наземні, повітряні і морські операції (бойові дії); антитерористичні операції; заходи з тилового та технічного забезпечення (логістика). Застосування елементів імітаційного моделювання дозволило оптимізувати процес навчання курсантів, а саме: підвищився рівень мотивації до вивчення військово-технічних дисциплін та рівень професійної компетенції військового спеціаліста.

Новим (відносно) явищем для системи освіти є застосування кейс-технології, як різновиду дистанційної технології навчання, заснованої на використанні наборів (кейсів) текстових, мультимедійних та аудіовізуальних навчально-методичних матеріалів та їх розповсюдження для самостійного вивчення при організації регулярних консультацій у викладачів традиційним або дистанційним способом (за допомогою системи MOODLE). Кейс-технологія, з одного боку, дозволяє здійснювати колективне навчання, з іншого – спрямована на індивідуальне самостійне (поглиблене) вивчення дисципліни.

Так на кафедрі тактики факультету бойового застосування військ НАСВ була впроваджена „Інформаційно-дистанційно-тренажерна система навчання”, яка розроблена фахівцями військової підготовки Сумського Державного Університету (м. Суми). Завдяки впровадженню її до процесу підготовки курсантів збільшено можливості доступу до навчальних матеріалів, оптимізації навчального режиму (теоретична частина – робота в режимі online з навчальним конвентом, практична частина – робота з інтерактивними тренажерами) та контролю за рівнем власного прогресу і результатів про виконання контрольних заходів.

Перелічені приклади і прийоми використання новітніх технічних засобів, приладів і систем дозволили створити на заняттях і навчаннях обстановку підвищеної емоційної напруженості, непередбачуваності дій і ситуацій, раптовості отримання завдань і варіативності умов для прийняття рішень щодо їх виконання (в обмеженому просторі, дефіциті часу, вночі і т. ін), напрацювати стереотипи адекватно реагувати і підвищити рівень професійної підготовленості курсантів.

Отже, на сучасному етапі розвитку суспільства в Україні відбуваються глибинні перетворення, які пов’язані з потребами інтеграції нашої держави до ЄС та набуття членства в Організації Північноатлантичного договору.

Особливо яскраво ці зміни спостерігаються в українській системі військової освіти, яка сприймає інновації, як невід’ємну частину для забезпечення захисту суверенітету і цілісності держави де головним показником сучасних змін є наближення її параметрів до рівня розвитку країн-членів НАТО.

Коваль І.О. (ВІТІ)
Симоненко О.А. (ВІТІ)
Троцько О.О. (ВІТІ)

ЗБЕРІГАННЯ ДАНИХ В CEPH FS З ВИКОРИСТАННЯМ ШЛЮЗУ CEPH RADOS

Актуальність сучасний стан розвитку сфери інформаційних технологій (IT) все більше спонукає до перенесення процесів безпеки ресурсів, складних обчислень, зберігання великих об’ємів даних, з класичних апаратних, серверних платформ на технології віртуалізації створення віртуального, тобто штучного, об’єкта чи середовища. Захист цінної інформації, що зберігається на віртуальних чи фізичних серверах – це пріоритет номер один як для організацій, так і для мереж передачі даних пунктів управління Збройних сил України.

Мета. Здійснити аналіз застосування шлюзу Ceph RADOS для зберігання даних в розподіленій файловій системі Ceph

Виклад основного матеріалу. Для того щоб уникнути втрати важливої інформації застосовуються розподілені файлові системи з захистом від збоїв. Розподілені файлові системи, які є паралельними і з захистом від збоїв, поділяють і реплікують дані на багато серверів для високої продуктивності і забезпечення цілісності даних.

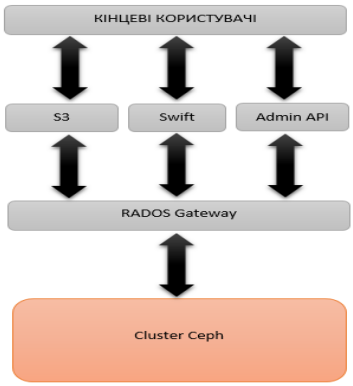


Рис.1 Система зберігання даних з використанням Ceph RADOS GATEWAY

Програмні бібліотеки Ceph надають клієнтським додаткам прямий доступ до об'єктно-орієнтованої системи зберігання RADOS, а також забезпечують основу для деяких розширених функцій Ceph, включаючи блоковий пристрій RADOS (RBD), шлюз RADOS (RGW) і файлову систему Ceph (CephFS). Кожен об'єкт зберігає дані, метадані та унікальний ідентифікатор. Оперативні системи не можуть безпосередньо звертатися до сховища об'єктів як до локальної або віддаленої файлової системи. Доступ до нього можна отримати тільки через API на рівні додатку. RADOS Gateway – це інтерфейс сховища об'єктів, створений librados для надання додатків шлюзу RESTful для кластерів RADOS. Шлюз RADOS підтримує два інтерфейси:

–S3-сумісний: забезпечує функціональність блочного сховища з інтерфейсом, сумісним з великою підмножиною Amazon S3 RESTful API.

–Swift-сумісний: забезпечує функціональність блочного сховища з інтерфейсом, сумісним з великою підмножиною OpenStack Swift API.

RADOS Gateway надає інтерфейси, сумісні з OpenStack Swift і Amazon S3, RADOS Gateway має власне управління користувачами. Він може зберігати дані в тому ж кластері RADOS, який використовувався для зберігання даних від клієнтів Ceph FS або блокових пристроїв RADOS. API S3 і Swift спільно використовують загальний простір імен, тому ви можете записувати дані з одним API і отримувати їх від інших.

Висновок. Представлений варіант застосування шлюзу Ceph Rados забезпечує для Ceph різні характеристики, що включають в себе розподілене зберігання об'єктів, високу доступність, надійність, самовідновлення та відсутність єдиної точки відмови.

Колесник В.В. (ВІТІ)

МЕТОД БАГАТОФАКТОРНОЇ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ НА ОБ'ЄКТАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Поступово все більшого поширення одержує багатофакторна ідентифікація, коли для визначення особистості застосовується відразу кілька параметрів. На сьогоднішній день одним з пріоритетних напрямків забезпечення інформаційної безпеки об'єктів різного призначення є удосконалення багатофакторних систем ідентифікації користувачів. Поряд з методами основаними на використанні матеріальних засобів (смарт-карти, магнітні карти і т.д.) все більшого застосування набувають біометричні методи ідентифікації (за відбитком пальця). Це пов'язано з підвищеними вимогами до інформаційної безпеки та існуючими вразливостями систем на основі матеріальних засобів ідентифікації (фізичний ключ може бути втрачений, викрадений тощо).

Пропонується здійснити розробку системи багатофакторної ідентифікації користувачів. Пріоритетним напрямком біометричної ідентифікації є розпізнавання обличь. Задача біометричної ідентифікації полягає в визначенні факту володіння об'єктом необхідною властивістю. У цьому методі ідентифікації будується тривимірний образ обличчя людини. На обличчі виділяються контури брів, очей, носа, губ і т.д., обчислюється відстань між ними і будується не просто образ , а ще безліч його варіантів на випадки повороту особи, нахилу, зміни виразу. Кількість образів варіюється залежно від цілей використання даного способу (для автентифікації , верифікації і т.д.). У задачі ідентифікації навчальна вибірка представляє собою множину об'єктів $M = \{x_i\}_i^n = 1$, кожен з яких або має властивість: $A(x_i) = 1$, $i = \overline{1,n}$ або ні.

З точки зору, вирішення задачі розпізнавання облич, необхідно, маючи два електронних зображення визначити, чи належать вони одній людини чи ні. Тобто, чи мають вони властивість належності одній людині:

$$A(x_1, x_2) = \begin{cases} 1, & x_1, x_2 \to x_i \\ 0, & x_1 \to x_i, x_2 \to x_j \end{cases}$$

На основі навчальної вибірки для: множини пар осіб $M = \{x_i, x_j\}_{i,j=1}^n$ необхідно побудувати ідентифікатор $L: R^n \to [0,1]$, який зможе визначати, чи має об'єкт необхідну ознаку чи ні.

З точки зору, вирішення задачі розпізнавання обличь, необхідно, маючи два електронних зображення визначити, чи належать вони одній людини чи ні. Тобто, чи мають вони властивість належності одній людині.

Одним з найпоширеніших методів розпізнавання обличь є використання нейронних мереж. До мережі надходять дані які отримані зі статистичного зображення, з отриманням даних відбувається порівняння з існуючими в базі даних зображень.

Створену систему біометричної ідентифікації на основі нейронної мережі можна використати для доповнення системи ідентифікації на основі матеріальних засобів, гібридні смарт-карти один чип підтримує контактний інтерфейс, інший - безконтактний.

Так, при спрацюванні фізичного ідентифікатора, активується модуль біометричної ідентифікації, за результатами роботи якого приймається рішення про допуск до об'єкту.

Механізм подвійної ідентифікації забезпечить покращений рівень безпеки на об'єктах військового призначення. Напрямком подальших досліджень є синтез оптимальної за структурою нейронної мережі для розпізнавання обличь та її програмна реалізація.

Колтовсков Д.Г. (ВІТІ)

МЕТОДИ ПОБУДОВИ РОЗВІД- ТА ЗАВАДОЗАХИЩЕНИХ КАНАЛІВ УПРАВЛІННЯ ТАКТИЧНИХ БпЛА

Актуальність, постановка задачі. Одним з основних завдань для безпілотних авіаційних комплексів (БпАК) тактичного призначення є проведення розвідувальних операцій районів, в яких отримання інформації звичайними засобами, включаючи авіарозвідку, ускладнене, або ж є небезпечним для життя військовослужбовців. Застосування комплексів тактичних безпілотних літальних апаратів (БпЛА) відкриває можливість оперативного способу отримання розвідувальної інформації різноманітних ділянок місцевості, періодичного спостереження заданих районів, цілезахвату, цілевказання та корегування вогню артилерії, забезпечення зв'язку та нанесення вогневих ударів по позиціям противника. Починаючи з 2014 року тактичні комплекси мікро- та міні-БпЛА набули широкого застосування в Збройних Силах України. БпАК, як правило, включають в себе оператора БпЛА, наземний пункт управління, безпосередньо БпЛА (один чи декілька) та канали зв'язку. Проте захисту каналів управління від зовнішніх впливів засобів радіоелектронної боротьби (РЕБ) та радіоелектронної розвідки (РЕР) супротивника, не дивлячись на зростання кількості інцидентів, не приділяється достатньої уваги. Атаки можуть бути спрямовані на перехоплення управління, виведення з ладу БпЛА, отримання розвідувальної інформації для подальшої атаки на оператора та системи, які з ним взаємодіють. Використання декількох каналів управління підвищує надійність системи передачі даних і в той же час є надлишковим з точки зору ефективного використання радіочастотного спектру. Одним із способів підвищення ефективності управління БпЛА є адаптація параметрів каналу управління БпЛА в залежності від умов розповсюдження сигналу та різній завадовій обстановці.

Мета. Метою роботи є дослідження методів побудови розвід та завадозахищених каналів управління тактичними БпЛА, що забезпечують достатній радіус дії каналів управління тактичними БпЛА в складних завадових умовах з забезпеченням необхідної швидкості обміну інформації між БпЛА та наземним пунктом управління.

Основні положення. Станом на початок російської збройної агресії проти України, Збройні сили України фактично не мали власних сучасних БпАК. Наявні на озброєнні Ту-141 „Стриж" були морально застарілі. Гостру потребу в безпілотних літаках-розвідниках спершу взялися задовольняти волонтери, адаптуючи цивільні апарати до вимог військових. Були створені, зокрема, БпЛА "Фурія", „Лелека-100", "PD-1".

Як показала практика використання БпЛА в бойових умовах експлуатації, одним з найслабкіших та уразливих місць є канал управління БпЛА. Під час виконання завдання за призначенням, використовуючи незахищений або недостатньо захищений канал управління БпЛА, відбуваються зрив виконання поставленого завдання або втрати БпЛА. В наслідок цього, в березні 2014 року у Криму був посаджений шляхом перехоплення каналу управління БпЛА армії США (MQ-5B Hunter зі складу 66-ї американської бригади військової розвідки, офіційно дислокованої в Баварії). Також широко відомий випадок захоплення повністю справного важкого БпЛА США в Ірані (в 2011 році був посаджений на території Ірану американський БпЛА RQ-170 Sentinel).

Для забезпечення достатніх показників розвід та завадозахищеності, пропускній здатності, ймовірності бітової помилки та забезпечення необхідної дальності зв'язку при передачі даних телеметрії з заданими швидкісними параметрами обміну інформації між БпЛА та наземними пунктами управління виникає потреба в більш глибокому дослідженні та використанні шумоподібних сигналів, спектрально-ефективних методів модуляції та застосуванні відповідних алгоритмів кодування сигналів. Дані методи призводить до підвищених показників „бюджету" каналу, високих показників чутливості приймачів по відношенню сигнал/шум на вході приймача, здатності детектування корисного сигналу

приймачем нижче рівня шумів, збільшення дальності дії радіосистеми, зменшення ймовірності бітової помилки, ускладнення детектування радіосигналу засобами РЕР супротивника за рахунок відносно малої потужності передавача.

Вибір робочого частотного діапазону роботи каналу управління тактичними БпЛА обумовлюється декількома факторами:

вимогами до маси та габаритів приймально-передавального обладнання та антен, що будуть встановлені на тактичні БпЛА, а також енергоефективності приймально-передавального пристрою тактичного БпЛА;

необхідної дальністю роботи при заданій ймовірності бітової помилки та заданими швидкісними параметрами обміну інформації між БпЛА та наземними пунктами управління;

можливістю отримання ліцензії на роботу в необхідному діапазоні або можливістю безліцензійної роботи.

Шумоподібні сигнали (широко використовуються в радіолокації та володіють достатніми показниками спектральних та кореляційних властивостей), що використовують внутрішньоімпульсну частотну модуляцію з лінійним законом змінення миттєвої частоти (ВЛЧМ) також широко використовують в сучасних військових бездротових сенсорних мережах WSNs (від англ. Wireless sensor networks). Висока енергетична скритність даних сигналів, що досягається розширенням смуги частот, як правило, набагато менша за потужність радіосигналів, що передаються на фіксованих частотах. Використання даного методу побудови розвід та завадозахищеного каналу управління тактичного БпЛА суттєво ускладнює виявлення даного каналу управління засобами РЕР супротивника, особливо в умовах дії вузькосмугових та широкосмугових перешкод з невідомими характеристиками. В таких умовах створення ефективних методів детектування наявності каналу управління тактичним БпЛА є досить складним завданням.

Для задач виявлення ВЛЧМ сигналів приймачем на борту тактичного БпЛА на фоні перешкод є критерій, за яким приймається рішення щодо детектування даного сигналу. Оскільки про властивості сигналу відомо лише те, що він багато разів в секунду змінює робочу частоту, то в якості подібного критерію можна використовувати детектування в заданій смузі частот кількох короткочасно використаних частотних імпульсів з близькими значеннями ширини спектра. Також важливою характеристикою при детектуванні корисного сигналу є знаходження автокореляційної функції ВЛЧМ сигналу, зв’язок якої з енергетичним спектром сигналу встановлюється інтегральними перетвореннями Фур’є. Передача інформаційних повідомлень по ВЛЧМ сигналах досягається шляхом скалярного добутку ортогональних сигналів в зазначеному спектрі. У результаті порівняння отриманих значень з пороговими значеннями формується рішення стосовно отримання інформаційного повідомлення з заданими показниками достовірності.

Використання ВЛЧМ сигналів для побудови розвід та завадозахищених каналів управління тактичними БпЛА дозволяє мінімізувати енергетичні затрати на забезпечення достатньої випромінюваної потужності передавачів та реалізувати можливість детектування корисного сигналу нижче рівня Гаусовського шуму, що в свою чергу підвищує показники розвід та завадозахищеності.

Висновки. Таким чином, на основі проведеного аналізу, було прийнято рішення про вибір методу для побудови розвід та завадозахищеного каналу управління БпЛА за рахунок використання шумоподібних ВЛЧМ сигналів. Але вибір даного методу побудови каналу управління тактичним БпЛА призводить до зменшення швидкості передачі телеметричної інформації від тактичного БпЛА на неземні пункти управління, тому напрямком подальших досліджень є створення методики підвищення швидкості передачі даних в завадозахищеному каналі керування тактичними БпЛА за рахунок управління параметрами ВЛЧМ сигналів.

к.т.н. Коновець В.І. Інститут Військово - Морських Сил НУ „ОМА” (м. Одеса)

ДЕЯКІ АСПЕКТИ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ З СЕНСОРАМИ У СКЛАДІ СИСТЕМИ СПОСТЕРЕЖЕННЯ ЗА НАДВОДНОЮ ОБСТАНОВКОЮ

Для захисту національних інтересів в морській сфері кожній з прибережних держав необхідно мати у своєму розпорядженні ефективні засоби для протидії можливим загрозам.

Потенційні загрози потрібно виявляти і розпізнавати якомога раніше і на максимальних дистанціях. Система морської ситуаційної обізнаності (Maritime Situational Awareness, MSA) покликана забезпечувати „Надання можливостей ... для досягнення ефективного розуміння ситуації на морі з метою підвищення ефективності планування та проведення операцій" [1].

Мета MSA: сприяти своєчасному і точному прийняттю рішень, що дозволяє вживати заходи для нейтралізації загроз інтересам національної безпеки.

Завдання технічних підсистем MSA: збір даних, інформаційне об'єднання, ”детектування аномалій”, візуальна аналітика і візуалізація. Основним продуктом MSA є: Визнана морська картина / Recognised Maritime Picture (RMP) – це візуалізація зображення морської діяльності у військово-морському контексті на електронному дисплеї. RMP компонується за даними активних і пасивних датчиків, що охоплює цікавий тривимірний простір, в якому всі виявлені морські контакти були оцінені за параметрами загрози і їм присвоєні категорія розпізнавання і номер треку [2]. Термін „визнаний” означає, що картина була оцінена до її розповсюдження. Центральний орган компілює та об’єднує дані з багатьох джерел та оцінює їхню дійсність. Структура RMP складається з виявлення об'єктів, що цікавлять, їх класифікації, оцінки того, що вони мають на увазі, та вирішення, чи потрібні будь-які подальші дії. RMP бажано будувати на основі всіх джерел даних, які можуть бути доступні у відношенні морського трафіка в області, що цікавить. Як правило, джерело даних буде надавати інформацію про місцезнаходження та ідентифікаційну інформацію про дане судно, і все частіше будуть залучатися уточнюючі дані, такі як: власник судна, вантаж та інша довідкова інформація. Всі ці дані, зібрані в картину, дають уявлення про обсяг, місце і характер судноплавної діяльності та служать основою для більш глибокого аналізу тенденцій і вразливостей. Об’єднання розрізнених наборів даних для створення RPM є все більш складним завданням через величезну кількість даних, доступних з усіх аспектів морської діяльності. Аналіз цих даних може виявляти аномалії, які вказують на загрозу, що представляє інтерес для осіб, які приймають рішення. Виявлення оманливої поведінки в морі стає схожим на спробу знайти голку в стозі сіна і закликає до використання розширених автоматичних і адаптивних інструментів для виявлення корисної інформації з даних.

Дані від датчиків -AIS, S-AIS, LRIT, VTS, VMS і ін. – основний канал інформаційного наповнення для MSA. Крім того, MSA спирається на джерела, які можуть забезпечити як дані на основі сенсорів, так і інші дані, не на основі сенсорів.

У загальних рисах, сенсорна система MSA повинна включати: сенсорну мережу, яка повинна бути достатню для підтримання належного рівня обізнаності та пов'язану з постійно оновлюваной і надійній базою даних; належну базу „типових моделей поведінки” (patterns of life – POL). Це важливо, щоб класифікувати цілі для конкретних областей і пір року, тобто слід вважати „звичайними”, „незвичайними” і „підозрілими”; інструмент аналізу, здатний обробляти, ідентифікувати і класифікувати ці „аномальні” поведінки, що вважаються релевантними для конкретних потреб; список адаптованих морських ситуаційних показників для виявлення підозрілої поведінки в межах їх областей інтересів. На поточному етапі розвиток системи MSA зв’язується з розширенням мережі сенсорів, збором даних та їх інформаційним об’єднанням. Детектування „аномалій”, візуальна аналітика стають ключовими інструментами для виявлення і виділення корисних знань з усе більшого обсягу доступної інформації про судна та їх переміщеннях на глобальному рівні. Автоматизація процесу виявлення структурованих аномалій, вдосконалення моделей поведінки суден є актуальними завданнями в подальшому поліпшенні морської ситуаційної обізнаності, розумінні того, що відбувається і може відбуватися в морі.

Коркін О.Ю. ВА (м. Одеса)
Дідик В.О. ВА (м. Одеса)
Симоненков В.М. ВА (м. Одеса)

ПОБУДОВА ЕФЕКТИВНИХ ІНФОРМАЦІЙНО-УПРАВЛЯЮЧИХ СИСТЕМ У СКЛАДІ НАЗЕМНИХ РОБОТИЗОВАНИХ КОМПЛЕКСІВ НА ПІДТРИМКУ МЕРЕЖЕЦЕНТРИЧНИХ СЦЕНАРІЇВ БОЙОВИХ ДІЙ

Оцінка досвіду бойових дій у локальних збройних конфліктах останніх років, насамперед, в зоні проведення операції Об'єднаних сил, свідчить про необхідність удосконалення існуючих систем управління й оперативного обміну тактичною інформацією та візуалізації бойової обстановки.

Одним із шляхів вирішення цих питань є широке впровадження завадозахищених автоматичних систем, які засновані на комплексному використанні глобальних навігаційних супутникових систем, систем електронної картографії й автоматичного цифрового радіозв'язку та передачі даних, у результаті об'єднання можливостей яких з'явилися реальні передумови створення принципово нових інформаційних систем та широкомасштабне застосування роботизованих засобів на підтримку мережецентричних сценаріїв бойових дій.

У зв'язку з цим корисно поглянути на підходи до побудови та шляхи розвитку подібних систем та засобів держав-членів НАТО з урахуванням новітніх технологічних викликів та погроз у сфері військової робототехніки [1].

За досвідом військових фахівців провідних країн світу вважається що саме мережецентрична концепція організації управління бойовими діями передбачає високий рівень оснащення збройних сил роботизованими засобами.

На сьогодні розробкою роботів військового призначення займаються понад сорок країн світу. Вже зараз існує ряд унікальних наземних бойових роботів, які наділені широким спектром можливостей, використовуються для ведення розвідки на полі бою та підтримки тактичних груп у складі бойових і розвідувальних підрозділів збройних сил США, Ізраїлю та Росії тощо.

В країнах-членах НАТО розробка, створення та розвиток наземних роботизованих засобів та відповідних технологій регламентуються низкою програмних документів, у яких головна увага приділяється питанням сумісності та підвищення рівня автономності під час застосування.

Слід зазначити, що наземний роботизований комплекс (НРК) – це, передусім, безпілотний наземний транспортний засіб (UGV, Unmanned Ground Vehicle – за термінологією НАТО) або наземна роботизована платформа (НРП) [2].

Системна архітектура, яка описує структуру й поведінку НРП, складається з низки технічних підсистем, засобів і програмних компонентів та інтерфейсів між ними. Зазвичай, така високорівнева архітектура передбачає наступні основні складові:

підсистема навігації (позиціонування), зв'язку та автоматизації управління;

транспортна підсистема;

бортова підсистема управління спеціальним обладнанням тощо.

До того ж, саме наявність достовірної навігаційної інформації визначає рівень автономності мобільного робота в просторі та обумовлює ефективність та функціональні можливості роботизованого засобу в цілому.

На цей час у ЗС України широко використовуються цифрові засоби радіозв'язку та передачі даних, які можуть безпосередньо підключатися до Ethernet-мереж та мають внутрішній GPS-приймач для відображення поточної позиції. Звіти про місцезнаходження сумісні зі стандартом НАТО STANAG 5527 FFTS (Friendly Force Tracking Systems, з англ. дружні системи відстеження) та відповідними системами управління бойовими діями, що використовуються в країнах-членів НАТО.

Наприклад, радіостанція одного з провідних виробників професійного обладнання радіозв'язку компанії „Harris" (США) RF-7850M-HH має внутрішній GPS-приймач для відображення поточної позиції та повідомлення свого місцезнаходження. Звіти про визначення поточної позиції передаються за допомогою UDP-протоколу у форматі, що включає дані MGRS (Military Grid Reference System, з англ. військова довідкова геокординатна система – геокоординатний стандарт, що використовується в НАТО), що містять інформацію про поточну позицію, зокрема, у форматі NMEA 0183 (IEC 61162-1), який визначає протокол обміну навігаційною інформацією між пристроями.

Однак, широке застосування систем супутникової навігації у військової сфері виявило низку недоліків. Причина тому – використання у супутникових навігаційних системах фазомодульованих сигналів, які вважалися найбільш захищеними від завад, але виявилось, що для руйнування сигналів супутникової навігації, досить випромінювати лінійно-частотні модульовані (ЛЧМ) імпульси в діапазоні частот від 9,4 до 44,5 МГц, які належать до категорії зосереджених перешкод, при цьому, потужність передавача може становити декілька ват.

На сьогодні у ряді країн світу розроблені та активно застосовуються зразки придушувачів сигналів супутникових навігаційних систем, що є серйозною загрозою застосуванню НРК на полі бою. Згідно аналітичним звітам, обладнання придушення й завад для GPS-навігації, яке пов'язане з Російською Федерацією, було застосовано в Сирії і Україні більше тисячі разів.

Прикладом вітчизняної розробки, яку було представлено на виставці „Зброя та безпека" у жовтні 2019 року ПАТ „Холдингова компанія „Укрспецтехніка" є комплекс „Анклав" призначений для створення перешкод для прийомних навігаційних систем GLONASS, GPS, BeiDou та Galileo, каналам управління та телеметрії, які використовуються БПЛА та іншим високоточним обладнанням, в радіусі до 20-40 км.

Тому, розробка вітчизняних НРК, а тим більше, створення автономних (напівавтономних) бойових наземних роботизованих засобів суттєво пов'язано з проблемою запобігання завадам супутникових навігаційних систем та є об'єктом ретельних досліджень.

Крім того, нещодавно представники армії США повідомили про експериментальне встановлення на легкі броньовані машини Stryker, Європейського командування США в Німеччині низки GPS-пристроїв з технологією проти завад в межах уявлення армії зразка 2028 року. Зі слів полковника Ніколаса Кіутаса, менеджера проекту MAPS (Mounted Assured PNT System, з англ. Приєднана гарантована система позиціонування, навігації і часової синхронізації) дана технологія розроблена для забезпечення надійного прийому навігаційних сигналів шляхом з'єднання приймача GPS з антеною проти завад.

У Науковому центрі Військової академії (м. Одеса) в рамках науково-дослідної роботи, шифр „Легіонер" проводяться дослідження щодо пошуку оптимального алгоритму динамічної регуляризації вибіркових оцінок кореляційної матриці спостережень за критерієм обчислювальної стійкості і спроможності [3], що в подальшому дозволить створити ефективну навігаційну систему з підвищеним рівнем перешкодозахищеності у складі НРК для потреб ЗС України.

ЛІТЕРАТУРА

1. C4ISR (C4ISR Products and Solutions). 2018. [Електронний ресурс] / Режим доступу: https://www.lockheedmartin.com/C4ISR (19.08.2018).

2. V.Skachkov, O.Efimchikov, O.Korkin and others, "Dynamic Regularization Parameter Optimization of a Sample Estimate of the Correlation Matrix of Observations by the Criterion "Computational Stability – Consistency""/ in Proceedings of the International Conf., 2nd IEEE Ukraine Conference on Electrical and Computer Engineering (UKRCON), pp. 18-23, 2019

Котюбін В.Ю. (в/ч А1906)
к.т.н. Романов О.М. (в/ч А1906)

АЛГОРИТМ ПОШУКУ ПЕРІОДУ ЦИФРОВОЇ ПОСЛІДОВНОСТІ НА ОСНОВІ СИНХРОННОГО НАКОПИЧЕННЯ

Актуальність Сучасні системи зв'язку та передачі даних (СЗПД) для забезпечення необхідної завадостійкості в каналі зв'язку використовують завадозахищене кодування (ЗК). Широкого розповсюдження через свою ефективність набули методи блокового кодування. При блоковому кодуванні для визначення періоду цифрової послідовності (ЦП), обумовленого додаванням до неї синхропослідовності (СП), і який може визначати вид і параметри кодування, розповсюдженим підходом є використання кореляційних властивостей ЦП.

Метою роботи є відшукання нових алгоритмів пошуку періодичностей у ЦП з блоковим ЗК в умовах часткової апріорної невизначеності виду і параметрів ЗК.

Основні положення. Аналіз алгоритмів пошуку періоду шляхом обробки локальних максимумів автокореляційної (АКФ) та взаємокореляційної функції (ВКФ) ЦП підтвердив працездатність алгоритмів на основі кореляційних функцій щодо визначення періоду ЦП. Час обчислення АКФ і ВКФ знаходиться в експоненціальній залежності від максимально можливого періоду ЦП, що перевіряється. Використання концепції найменшої кількості звернень до масиву, багатоядерності сучасних процесорів та використання зсуву покажчиків елементів ЦП для розрахунку кореляційних функцій дозволило значно скоротити час пошуку періоду ЦП.

У ході дослідження запропоновано новий алгоритм пошуку періоду ЦП на основі поекземплярного порівняння та синхронного накопичення ЦП. Його суть полягає накопиченні на початковому етапі алгоритму певної довжини ЦП $s(n)$ та в подальшому її розбитті на q ЦП $s_0(n), s_1(n), ..., s_{q-1}(n)$, що слідують одна за одною у часі, однакової довжини $l = T_{min}$. У такому випадку накопичену вхідну послідовність $s(n)$ можна преставити у вигляді матриці:

$$l = \begin{pmatrix} s_{0,0} & s_{0,1} & \vdots & s_{0,T-1} \\ s_{1,0} & s_{1,1} & \vdots & s_{1,T-1} \\ \cdots & \cdots & \cdots & \cdots \\ s_{q-1,0} & s_{q-1,1} & \vdots & s_{q-1,T-1} \end{pmatrix}$$

Для пошуку періоду необхідно попередньо задати значення l, яке на початковому етапі циклу дорівнюватиме мінімально можливому періоду ЦП та застосувати до нього формулу (1):

$$R(l) = \frac{1}{l} \sum_{n=0}^{l-1} \prod_{u=0}^{q-1} s_u(n), \qquad (1)$$

де символом П позначено виконання побітної логічної операції "еквівалентність".

В результаті на кожній ітерації поекземплярного порівняння ЦП (побітного відшукання) q $s_0 \equiv s_1 \equiv s_2 \equiv ... \equiv s_{q-1}$ одиничне значення буде отримане лише за умови рівності всіх бітів стовпця, що відповідає сталій СП. Кількість отриманих одиниць підсумовується по всій довжині ЦП l та нормується до неї.

Довжина l ЦП $s_0(n), s_1(n), ..., s_{q-1}(n)$ збільшується на крок Δl (як правило, $\Delta l = 1$) і описана послідовність дій повторюється, поки значення l не досягне максимально можливого періоду ЦП T_{max}.

Очевидно, для коректного проведення обчислень, необхідно накласти обмеження $L \geq qT_{max}$.

В отриманій залежності $R(l)$ здійснюється пошук максимального значення. Найменше значення l, при якому досягається максимум $R(l)$, відповідає шуканому періоду T. Більші значення l, при яких досягається максимум $R(l)$, відповідають кратним значенням періоду: $2T$, $3T$ ... і можуть бути використані для підтвердження знайденого значення істинного періоду T. Алгоритм, який відображає описану послідовність дій, представлений на рис. 1.

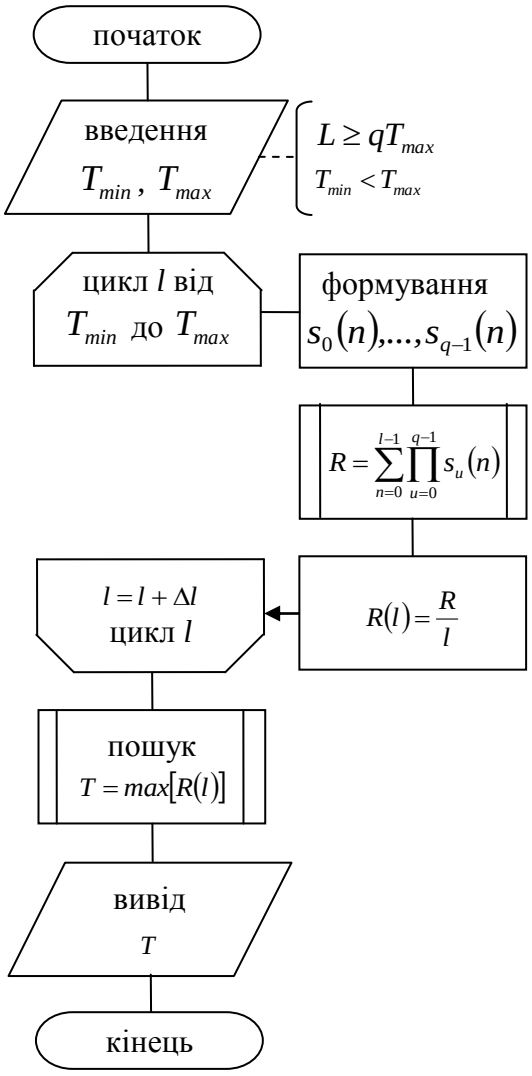


Рис. 1. Алгоритм пошуку періодичності ЦП на основі синхронного накопичення

Висновки. Запропонований алгоритм найбільш близько відображає процес евристичного підходу при пошуку періоду ЦП і забезпечує отримання достовірних результатів.

Основними перевагами запропонованого алгоритму є простота реалізації та швидкість роботи алгоритму, що дозволяє достатньо точно вирішити задачу пошуку періоду у ЦП з блоковим ЗК.

До його недоліків слід віднести:

в десятки разів більший об'єм даних, що аналізуються порівняно з пошуком на основі АКФ/ВКФ, і, відповідно, обчислювальних операцій;

не вирішеним залишається питання в мінімально необхідній кількості накопичених вхідних даних.

Кротов В.Д. (ВІТІ)

АНАЛІЗ ПІДХОДІВ МОДЕЛЮВАННЯ ТРАФІКА З ТОЧКИ ЗОРУ ВІДПОВІДНОСТІ МЕРЕЖАМ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ

Організація управління системою управління військами та озброєнням під час ведення бойових дій, які характеризуються гібридним способом її проходження та наявністю великої кількості різнорідної за своїм фізичним змістом інформації, вимагає повної та своєчасної поінформованості відповідних посадових осіб відносно ситуації, яка складається на полі бою. Саме тому в тактичній ланці управління військами збір, зберігання, обробка, поширення та надання своєчасного управлінського рішення можливі лише шляхом використання сучасних мобільних радіомереж, які відносяться до класу MANET.

Створення адекватних аналітичних моделей в області мобільних Ad-Hoc мереж, зв'язане зі значними труднощами, що пов’язані з тим, що на процес передачі даних в цих мережах впливає велика кількість різних чинників, які носять випадковий характер і слабо піддаються строгому математичному аналізу.

Сучасні теоретичні методи і підходи опису процесів в інформаційних системах і мережах різноманітні і вимагають наукового осмислення для застосування на практиці. Все більшого значення набувають теоретико-ймовірнісні методи досліджень, засновані на імовірнісному трактуванні процесів, що протікають в інформаційних системах. Статистичний підхід дозволяє більш повно врахувати стан динамічної системи, характер управляючих дій, результуюча поведінка інформаційних потоків у мережах і у багатьох випадках адекватніший для вирішення різних практичних завдань.

Коло проблем вказаного підходу досить широке: опис математичних моделей випадкових процесів в інформаційних системах, формування на їх базі статистичних методів перевірки гіпотез і виявлення, оцінювання і фільтрації, інтерполяції (згладжування) і екстраполяції (прогнозування), а також розробка алгоритмів оптимального управління стохастичними системами. Основними критеріями при виборі теоретичного підходу моделювання мережі є наступні: модель має бути придатної для опису мережі; модель має бути універсальною, тобто мережі, що адаптується до різних фрагментів; точність відповідності реальним потокам даних має бути не більше 10 % при прийнятній обчислювальній громіздкості; модель має бути придатної для прогнозування поведінки мережі при інтенсивнішому трафіку; модель повинна відображати маршрути трафіку і їх зміну. Для того, щоб визначити, який з теоретико-ймовірнісні методів найбільш близький до поведінки мереж тактичної ланки управління, і необхідно виконати порівняльний аналіз. Іншими словами, потрібна додаткова перевірка пропонованих підходів, заснована на даних виміру трафіка реальних мереж.

Метою роботи є проведення порівняльного аналізу теоретичних підходів моделювання мережевого трафіка для розробки основних етапів моделювання трафіка мереж тактичної ланки управління.

Для досягнення мети необхідно вирішити наступні завдання:

1. Провести аналіз теоретичних підходів до моделювання трафіка.

2. Показати принципи і основні етапи технології моделювання трафіка комерційних мереж.

3. Обґрунтувати необхідність застосування комбінованого підходу для статистичного опису трафіка мережі.

Висновки. В результаті проведених досліджень стають ясними принципи і основні етапи технології моделювання трафіку мереж. Важливим виводом з проведеного аналізу є необхідність застосування комбінованого підходу для статистичного опису трафіку мереж.

Подальший напрям дослідження спрямований на досягнення найкращої точності моделі на основі не лише вивчення статистичних властивостей реального трафіка мережі , що постійно змінюється.

к.т.н. Кубрак О. М. (ЖВІ)

ПРОГРАМНО-АПАРАТНІ ЗАСОБИ ОБРОБКИ РАДІОСИГНАЛІВ ТА ФОРМУВАННЯ РАДІОПЕРЕШКОД

Актуальність. Як показує досвід останніх воєнних конфліктів та воєн, зокрема в Грузії, Сирії та на сході України, ведення радіоелектронної боротьби стало невід'ємною частиною бойових дій (операцій).

Це зумовлено застосуванням радіоелектронних засобів (РЕЗ) при виконанні завдань із розвідки та управління в електромагнітному просторі.

Завданням дослідження є запропонувати варіант модернізації існуючих станцій перешкод, гнучкість яких буде забезпечена за рахунок використання спеціальних обчислювальних засобів які будуть реалізовувати сучасні (нові) алгоритми оцінювання, аналізу та розпізнавання (ідентифікації) прийнятих радіосигналів, а також формування різних видів перешкод.

Основні положення. З метою руйнування або введення хибних даних в радіоканали систем добування інформації, управління військами та зброєю безперервно удосконалюються засоби радіоелектронної боротьби для забезпечення переваги в електромагнітному просторі.

На сучасному етапі, для обробки сигналів частіше за все використовуються класичні алгоритми аналізу, наприклад алгоритм перетворень Фур'є для проведення спектрального аналізу, метод смугових фільтрів, метод порівняння, які реалізовані на базі аналогової апаратури.

При цьому наприклад, роздільна здатність за частотою визначається в основному і обмежена часом спостереження (аналізу) вхідного радіосигналу, що суттєво ускладнює якість обробки або взагалі робить її неможливою при аналізі короткочасних сигналів, зокрема аналіз радіосигналів систем зв'язку з послідовною перестройкою радіочастоти.

Відомо ряд сучасних алгоритмів оцінювання параметрів радіосигналів (MUSIC, Кейпона, Берга, Прони та інші), які дають можливість здійснювати більш якісний аналіз радіосигналів, тобто при високій (надрелеєвській) роздільній здатності за частотою, забезпечується можливість оцінювання амплітуди, частоти, фази, часових параметрів короткочасних (малих за тривалістю) радіосигналів в порівнянні з алгоритмом дискретного перетворення Фур'є.

В даний час розроблено ряд алгоритмів обробки, аналізу, розпізнавання та формування сигналів, які здатні забезпечити виконання певних задач та сучасних вимог до станції перешкод.

В доповіді пропонується варіант реалізації цифрової адаптивної станції радіоперешкод шляхом застосування спеціальних обчислювальних пристроїв та нових алгоритмів (програм) оцінювання параметрів радіосигналів з метою визначення пеленгів на джерела радіовипромінювання, розпізнавання РЕЗ та формування квазіоптимальних радіоперешкод для їх радіоелектронного подавлення.

Показано послідовність обробки прийнятого радіосигналу ДРВ, формування радіоперешкоди, управління та індикації результатів виконання завдань.

Висновки. На обговорення виноситься структурна схема цифрової адаптивної СРП та принцип її функціонування.

Наводиться перелік алгоритмів обробки та оцінки параметрів радіосигналів, радіопеленгування ДРВ та ідентифікації РЕЗ, прийняття рішення, а також формування радіоперешкод. Пояснюється їх суть та особливості практичної реалізації.

д.т.н. Кувшинов О. В. (НУОУ)
Зотова І. Г. (НУОУ)
Боголій С.М. (ВІТІ)

СИНТЕЗ ВИСОКОЕФЕКТИВНИХ СИГНАЛЬНО-КОДОВИХ КОНСТРУКЦІЙ З ТУРБО-КОДАМИ

Проблеми синтезу ансамблів сигналів і алгоритмів їх формування та приймання, що забезпечують обробку інформації в реальному часі і досягнення ймовірнісно-енергетичних характеристик, близьких до граничних характеристик пропускної здатності за Шенноном, є актуальними при створенні систем передачі інформації.

Відомі конструктивні процедури формування ансамблів сигналів, близьких до оптимальних за метричними характеристиками, засновані на використанні теорії завадостійких кодів. Такі ансамблі сигналів мають ряд корисних властивостей, з їх використанням розроблені алгоритми оптимального та підоптимального приймання. Найбільш відомими з даного класу є ансамблі сигналів на основі згорточних кодів. Так, алгоритм оптимального приймання Вітербі реалізує критерій мінімальної помилки при прийманні дискретних повідомлень.

При наближенні до ймовірнісних характеристик, близьких до характеристик шеннонівської пропускної здатності, алгоритм Вітербі характеризується надмірною складністю реалізації. Альтернативою відомим ансамблям сигналів за складністю реалізації алгоритмів їх формування та обробки є сигнально-кодові конструкції з турбо-кодами. До принципових аспектів турбо-кодів відносяться наступні:

а) при формуванні турбо-кодів використовується сукупність простих згорточних або блокових кодів;

б) на приймальному боці застосовують ітеративне посимвольне приймання, основу якого становлять процедури обчислення апостеріорних ймовірностей символів дискретних повідомлень;

в) складність ітеративного прийому турбо-кодів визначається складністю процедур посимвольного прийому складових кодів і практично не залежить від тривалості сигналів у складі турбо-кодів.

Проведено дослідження розроблених процедур ітеративного приймання турбо-кодів, які формуються шляхом паралельного і послідовного включення блокових кодів. Дослідження показують, що даний клас турбо-кодів має більше високі імовірнісні характеристики, ніж турбо-коди на основі паралельного включення згорточних кодів. Для запропонованих блокових кодів розроблено алгоритми оптимального посимвольного приймання на основі алгоритмів спектрального перетворення в узагальненому базисі Віленкина-Крестенсона. Для двійкових сигналів основу алгоритмів оптимального посимвольного приймання становить алгоритм швидкого спектрального перетворення в базисі Уолша-Адамара. Розмірність базису Уолша-Адамара (і відповідно складність реалізації процедур приймання) визначається розмірністю перевірочних матриць.

Проведено порівняння за кількістю арифметичних операцій розроблених алгоритмів стосовно відомого алгоритму обчислення апостеріорних ймовірностей символів MAP (maximum a posteriori probability), а також його модифікацій. Алгоритм MAP застосовується для згорточних кодів, характерною властивістю яких є симетрична ґратчаста структура породжувальних матриць.

За результатами імітаційного моделювання можна зробити висновок про те, що запропоновані алгоритми мають характеристики завадостійкості, близькі до характеристик оптимальних алгоритмів посимвольного приймання (втрати менш 0,5 дБ), але значно меншу обчислювальну складність (в 3,2-4,6 рази).

д.т.н. Кузавков В.В. (ВІТІ)
Зарубенко А.О. (ВІТІ)

МЕТОДИКА СИНТЕЗУ ЦИФРОВОГО КОРЕКТУЮЧОГО ПРИСТРОЮ СИСТЕМИ АВТОМАТИЧНОГО УПРАВЛІННЯ ПОЛОЖЕННЯМ ПЛАТФОРМИ АНТЕННОГО ПОЛЯ МОБІЛЬНОЇ БАЗОВОЇ СТАНЦІЇ

З метою підвищення ефективності використання сукупності засобів радіо- та супутникового зв'язку, які розташовано локально із забезпеченням вимог електромагнітної сумісності – запропоновано використовувати спеціальну керовану платформу з антенними системами засобів зв'язку. Система автоматичного управління (САУ) платформою антенного поля (АП), яка встановлена на транспортному засобі, повинна бути: швидкодіючою, високоточною та надійною. Виконання зазначених вимог до проектної САУ потребує її синтезу та дослідження. Запропоновано вирішення часткової задачі синтезу САУ – синтез коректуючого пристрою (КП), яка полягає у визначенні схеми і параметрів КП на основі відомої структури і параметрів основних функціонально необхідних елементів САУ.

Розробка КП, на базі цифрової техніки є **актуальним завданням** оскільки незмінна структура САУ повинна задовольняти низці показників.

Отже, необхідно визначити схему і параметри КП, включення якого в систему забезпечить отримання необхідних показників якості, а саме: величини перерегулювання та помилки в сталому режимі.

Якість перехідного процесу (як характеристики САУ) оцінено інтегральним критерієм (дозволить отримати загальну оцінку показників якості аперіодичних і коливальних процесів), який називається квадратичною інтегральною оцінкою:

$$J = \int_0^\infty [\theta_n(t)]^2 dt, \qquad (1)$$

де $\theta_n(t)$ – помилка при відпрацюванні ступеневого впливу.

Інженерні методи синтезу КП – поступаються запропонованій методиці за кількістю операцій, наочності, оперативності оскільки заснована на широкому використанні ЕОМ.

При використанні цифрового коректуючого пристрою (ЦКП) для корекції динамічних властивостей САУ – пропонується наступний порядок:

1. знаходження логарифмічної амплітудної і фазової частотних характеристик та перехідної функції об'єкта регулювання, замкнутого зворотнім зв'язком;
2. проведення вибору варіантів ЦКП і виконання оптимізації параметрів обраного варіанту структури КП по заданому (обраному) критерію якості;
3. знаходження часових та частотних характеристик оптимізованої САУ з обраним варіантом ЦКП та оцінювання результатів корекції.

Для отримання часових характеристик перехідного процесу в системах використовується алгоритм з програмною реалізацією. У кожній точці на графіку перехідного процесу обчислюється значення інтегрального критерію (1). Після закінчення перехідного процесу, коли $\theta(t) \le 0{,}1\%$, числове значення інтегрального критерію якості і графік перехідного процесу реєструється (виводяться на друк).

Висновок. При моделюванні САУ на ЕОМ доцільно використовувати числові методи. Запропонована методика визначення дискретних частотних характеристик тракту з ЦКП, заснована на опису цього пристрою в часовій області системою різницевих рівнянь, проста і має високу точність (похибка обчислень $\le 3\%$). Відрізняється від методів заснованих на зв'язку перехідної функції системи з дійсною частотною і логарифмічною амплітудною характеристиками, можливістю синтезу САУ з необхідними показниками якості безпосередньо по параметрах перехідної функції. При знаходженні, як частотних, так і часових характеристик використовується одна і та ж математична модель пристрою в часовій області – система різницевих рівнянь.

проф. Кузнецов О.О., Ковальчук Д. Ю., Дьяченко А.С., Сафоненко В.Е., Даценко С.С.
(Харківський національний університет імені В. Н. Каразіна)

ШВИДКОДІЯ АЛГОРИТМІВ ГЕШУВАННЯ, ПРИДАТНИХ ДЛЯ ВИКОРИСТАННЯ В БЛОКЧЕЙН-МЕРЕЖАХ

Актуальність. В основі технології блокчейн лежить формування безперервного послідовного ланцюжка блоків, який надійно зв'язує збережену інформацію. Копії ланцюжків блоків, як правило, зберігаються на безлічі різних комп'ютерів незалежно один від одного, що забезпечує безпечне та стійке до зміни зберігання інформації. Для побудови зв'язаних списків блоків використовують гешування. Це спеціальний криптографічний примітив, що забезпечує одностороннє, стійке до колізій і пошуку прообразів обчислення геш-кодів (дайджестів повідомлення). Отже, вивчення властивостей функцій гешування, які застосовуються (або можуть застосовуватися) в сучасних децентралізованих блокчейн системах, є важливим та актуальним.

Мета. Метою роботи є дослідження та порівняння швидкодії криптографічного гешування на різних обчислювальних системах. Для цього оцінюється кількість тактів обчислювальної системи на один байт (Cycles/byte), обсяг гешованого повідомлення за одну секунду (MB/s) та кількість сформованих геш-кодів за секунду (KHash/s). Додатково проводяться дослідження швидкодії окремих криптографічних функцій гешування на графічних обчислювачах.

Основна частина. В цій роботі розглядаються найбільш поширені та застосовувані алгоритми криптографічного гешування, які стандартизовані на міжнародному та національному рівнях, а також алгоритми, які хоча і не стандартизовані, але застосовуються у більшості сучасних децентралізованих системах, побудованих за технологією блокчейн. Зокрема, досліджено наступні функції криптографічного гешування:

– сімейство криптографічних алгоритмів ARGON (геш-функції ARGON2D та ARGON2I);

– алгоритм гешування BALLOON;

– сімейство криптографічних алгоритмів BLAKE (геш-функції BLAKE224, BLAKE256, BLAKE384, BLAKE512);

– сімейство криптографічних алгоритмів BMW (геш-функції BMW224; BMW256; BMW384; BMW512);

– сімейство криптографічних алгоритмів CUBEHASH (геш-функції CUBEHASH224; CUBEHASH256; CUBEHASH384; CUBEHASH512);

– алгоритм гешування DJB-2;

– сімейство криптографічних алгоритмів ECHO (геш-функції ECHO224; ECHO256; ECHO384; ECHO512);

– алгоритм гешування ED2K;

– сімейство криптографічних алгоритмів EDONR (геш-функції EDONR256; EDONR512);

– алгоритм гешування DAGGER-HASHIMOTO та його подальший розвиток і вдосконалення – алгоритм ETHASH;

– сімейство криптографічних алгоритмів FUGUE (геш-функції FUGUE224; FUGUE256; FUGUE384; FUGUE512);

– алгоритм криптографічного гешування GOST34.11-94-256;

– сімейство криптографічних алгоритмів GROESTL (геш-функції GROESTL224; GROESTL256; GROESTL384; GROESTL512);

– сімейство криптографічних алгоритмів HAMSI (геш-функції HAMSI224; HAMSI256; HAMSI384; HAMSI512);

– алгоритм гешування Has160;

– сімейство криптографічних алгоритмів J-H (геш-функції J-H224; J-H256; J-H384; J-H512);

– сімейство криптографічних алгоритмів KECCAK (геш-функції KECCAK224; KECCAK256; KECCAK384; KECCAK512, які стандартизовані як SHA3);

– алгоритм гешування Kupyna (геш-функції Kupyna256 та Kupyna512);

– алгоритм гешування LOSELOSE;

– сімейство криптографічних алгоритмів LUFFA (геш-функції LUFFA224; LUFFA256; LUFFA384; LUFFA512);

– сімейство криптографічних алгоритмів LYRA (геш-функції LYRA2RE; LYRA2REV2);

– сімейство криптографічних алгоритмів MD (геш-функції MD4 та MD5);

– алгоритм криптографічного гешування PANAMA256;

– алгоритм гешування PROGPOW;

– алгоритм криптографічного гешування RIPEMD160;

– алгоритм криптографічного гешування SCRYPT;

– алгоритм криптографічного гешування SHA1;

– сімейство криптографічних алгоритмів SHA2 (геш-функції SHA2-256 та SHA2-512);

– сімейство криптографічних алгоритмів SHABAL (геш-функції SHABAL256 та SHABAL512);

– сімейство криптографічних алгоритмів SHAVITE (геш-функції SHAVITE224; SHAVITE256; SHAVITE384; SHAVITE512);

– сімейство криптографічних алгоритмів SIMD (геш-функції SIMD224; SIMD256; SIMD384; SIMD512);

– сімейство криптографічних алгоритмів SKEIN (геш-функції SKEIN224; SKEIN256; SKEIN384; SKEIN512);

– алгоритм гешування SNEFRU256;

– алгоритм гешування STREEBOG (у варіантах STREEBOG256 та STREEBOG512);

– алгоритм гешування TIGER;

– алгоритм гешування WHIRLPOOL;

– алгоритми гешування із сімейства «X» (алгоритми X11; X12; X13; X14; X15; X17).

Розглянуті алгоритми гешування побудовано за різними схемами обробки інформаційних повідомлень та із застосовуванням різних математичних перетворень блоків даних для обчислення геш-кодів. Різна ідеологія побудови зазначених алгоритмів обумовлена міркуваннями авторів-дослідників та їх суб'єктивними уявленнями про раціональну побудову функції гешування за критеріями стійкість/складність. Нашу увагу зосереджено, перш за все, на можливості застосування досліджених алгоритмів при побудові децентралізованих блокчейн-систем, зокрема, криптовалют, проектів розподілених технологій, смарт-контрактів, тощо.

Висновок. Більшість проектів розподілених мереж використовує надійні та перевірені часом алгоритми криптографічного гешування (наприклад, алгоритми KECCAK, SHA2, RIPEMD160, тощо), які володіють відносно високими швидкісними показниками. Але останніми роками для захисту від ASIC-майнерів почали застосовуватися і інші геш-функції, які хоча і можуть бути навіть швидшими за KECCAK, SHA2 або RIPEMD160, але володіють певними вадами стосовно властивостей необоротності. Як приклад можна навести застосування алгоритмів MD4, EDONR-256, EDONR-512, ED2K, або навіть найпростіших функцій DJB-2 та LOSELOSE. Отримані результати порівняльного аналізу дають можливість обирати криптографічні функції гешування за критеріями швидкодії на різних пристроях та обґрунтовувати їх практичне застосування для побудови децентралізованих систем типу блокчейн. Це також стосується і результатів порівняльного аналізу швидкодії на графічних обчислювачах, особливо з приводу можливої розбудови національного сегменту блокчейн-мереж.

к.е.н. Леонтович С.П.(НУОУ)
(ORCID: 0000-0002-0393-1869)

ПОГЛЯДИ НА НАПРЯМИ АВТОМАТИЗАЦІЇ ПРОЦЕСІВ РОЗРАХУНКІВ ІЗ ЛОГІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ ЗБРОЙНИХ СИЛ

Актуальність, постановка задачі. З того часу, як відбулася окупація з наступною анексією Росією українського Криму та розпочалась збройна агресія Росії проти України на Донбасі, загострилось питання розвитку Збройних сил України їх спроможностей, у тому числі із забезпечення. Стратегічним оборонним бюлетенем визначено, відсутність ефективної об'єднаної системи логістики, яка здатна підтримувати роботу всіх складових сил оборони, відсутність автоматизованої системи управління у сфері матеріально-технічного забезпечення [1]. Погляди, щодо вирішення окремих питань з формування автоматизованої системи управління логістичним забезпеченням та пропозиції з їх розв'язання, висвітлюються у різних джерелах [2 – 4].

Поряд з цим, автоматизована підтримка процесів здійснення розрахунків щодо забезпечення військ (сил) озброєнням, військовою технікою (ОВТ), інших питань матеріально-технічного забезпечення (МТЗ), як складова перспективної автоматизованої системи управління логістичним забезпеченням, є одним з кроків підвищення якості та оперативності роботи органів військового управління (ОВУ). Таке підвищення ефективності роботи ОВУ логістики впливатиме на набуття Збройними Силами визначених спроможностей, підвищення рівня їх боєздатності, яке обумовлює актуальність і наукову значущість роботи, що висвітлюється у даних тезах.

Мета. Визначення поглядів на напрями автоматизації процесів розрахунків із логістичного забезпечення Збройних Сил.

Основні положення. Активізація бойових дій та інші чинники загострюють актуальність підняття рівня боєздатності, зокрема, за рахунок автоматизації системи управління із забезпеченням Збройних Сил України.

Значимість вирішення цих питань знаходить своє підтвердження під час виконання завдань з забезпечення бойових дій на сході України у антитерористичній операції та операції об'єднаних сил. Завданнями 1.4.6 і 1.4.8 Матриці досягнення стратегічних цілей і виконання основних завдань оборонної реформи визначено впровадження автоматизованої системи управління оборонними ресурсами сил оборони відповідно до стандартних угод НАТО (STANAG), створення єдиної інформаційної системи управління оборонними ресурсами, матеріально-технічним забезпеченням та іншими видами забезпечення.

Передовий досвід провідних країн світу, зокрема членів НАТО, наводить приклади розробки сучасних інформаційних систем матеріально-технічного забезпечення військ.

Так, у Збройних Силах Сполучених Штатів Америки розроблені наступні інформаційні системи (Табл. 1) для забезпечення військових формувань [5].

Таблиця 1

Назва системи	Призначення систем
(Tc-Aims Ii) Transportation Coordinators' Automated Information For Movement System Ii	Система транспортного забезпечення
GTN (Global Transportation Network)	Глобальна мережа управління перевезеннями
BCS3 (Battle Command Sustainment Support System)	Автоматизована система управління тилом
ECSS (Expeditionary Combat Support System)	Управління експедиційними силами
AMT (Asset Marking and Tracking)	Відстеження тилових ресурсів (автоматична ідентифікація і радіочастотне маркування)
EVTI (Enterprise Vehicle Transformation Initiative)	Система модернізації парку бойових і забезпечуючих машин
TEMP (Tactically Expandable Maritime Platform)	Модулі на основі стандартних морських контейнерів
LOGCAP (Logistic Civil Augmentation Program)	Залучення цивільних організацій для тилового забезпечення ЗС
ERP SAP (Systems, Applications and Products) R/3	Система тилового забезпечення
GCSS-A (Global Combat Support SystemArmy)	Глобальна АСУ тиловим забезпеченням Сухопутних Військ
GCCS-AF (US Air Force)	Глобальна система управління повітряних сил
GCCS-M (US Navy/Marine Corps)	Глобальна система управління ВМС і морської піхоти

GCCS-J (Joint Command Centers)	Глобальна система управління власною системою управління збройних сил
DPAS (Defense Property Accountability System)	Система управління запасами
FEDLOG (Federal Logistics)	Федеральний каталог
DSS (Distribution Standard System)	Стандартна система розподілу
PD2 (Procurement Desktop-Defense)	Забезпечення закупівель
CSSCS (Combat Service Support Command System)	АСУ тилом армійського корпусу
BEA-Log (Business Enterprise Architecture - Logistics)	АІС тилового забезпечення МО
AKM (Army Knowledge Management)	АСУ управління знаннями
FBCB2 (Force XXI Battle Command Brigade and Below)	АСУ тактичної ланки рівня бригади і нижче
CLOE (Common Logistics Operating Environment)	Єдина інформаційна середа тилового забезпечення
LDSS (Logistics Decision Support System)	Система підтримки прийняття рішень з постачання рівня батальйону і нижче

На сьогодні, у наслідок відсутності у Збройних Силах подібних систем на тактичному, оперативному і стратегічному рівні, ОВУ логістики не мають змоги на високому рівні ефективності управляти матеріально-технічними засобами, вести автоматизований облік військового майна, контролювати його рух. Практично всі процеси управління логістичним забезпеченням здійснюються у ручному режимі з мінімальною автоматизацією.

Зрозуміло, що розробка перспективної єдиної системи управління логістичним забезпеченням Збройних Сил потребуватиме значних фінансових ресурсів та часу, проте автоматизація процесів розрахунків щодо ОВТ, МТЗ, інших ресурсів, дозволить значно підняти ефективність роботи ОВУ та логістичного забезпечення у цілому.

Тому, актуальним є завдання створення у найближчий час у складі перспективної єдиної системи управління логістичним забезпеченням модулів автоматизованих розрахунків із логістичного забезпечення, з подальшим (протягом року) врахуванням складу функціональних груп спроможностей забезпечення (SUSTAIN) кодів Єдиного переліку (Каталогу) спроможностей Міністерства оборони України та Збройних Сил України [6].

З метою обґрунтування напрямів автоматизації процесів здійснення розрахунків із логістичного забезпечення Збройних Сил, запропоновано розв'язання основних розрахункових завдань логістики на трьох рівнях військового управління.

На **тактичному** рівні пропонується автоматизація основних розрахунків із логістичного забезпечення за наступними процесами: узагальнення інформації за наявні запаси ОВТ і МТЗ; порівняння їх з діючими нормами та визначення потреби; формування заявки (звіту) у довольчий орган забезпечення; облік отриманого ОВТ і МТЗ; формування пропозицій по розподілу ОВТ і МТЗ за завданнями та підрозділами, формування документів на видачу; розрахунок планових заходів техобслуговування відносно напрацювання ОВТ та обладнання; формування бази даних та документів на списання нестач та бойових втрат.

На **оперативному** рівні пропонується автоматизація основних розрахунків із забезпечення за наступними процесами: визначення потреб в ОВТ і МТЗ за військові частини; формування пропозицій і документів на їх перерозподіл, видачу; формування заявок (звітів) на забезпечення; опрацювання, узагальнення звітів, донесень про рух ОВТ і МТЗ. На **стратегічному** рівні пропонується автоматизація основних розрахунків із забезпечення за наступними процесами: проведення розрахунків за військові частини оперативного рівня, центри забезпечення, бази; визначення їх потреб у поточному і довгостроковому забезпеченні; формування плануючих документів, пропозицій по логістичному забезпеченню підлеглих формувань; ведення обліку з отриманого ОВТ і МТЗ від промисловості, виробників; формування пропозицій по забезпеченню підрозділів у міжнародних навчаннях, місіях ООН і НАТО; формування бази даних з нестач та бойових втрат. Автоматизація на трьох рівнях управління процесів здійснення розрахунків з логістичного забезпечення ЗС дозволить:

проводити розрахунки у розрізі розрахунково-постачальних одиниць та коштах наявного та потрібного за встановленими нормами накопичення ОВТ та МТЗ для військової частини (з'єднання);

швидко обробляти інформацію та опрацьовувати необхідні розрахунки, деталізувати плани логістичного забезпечення відповідного рівня;

оперативно і якісно формувати розрахунки, зокрема потреб доставки ОВТ та МТЗ, наприклад, при зміні чисельності особового складу або норм витрат та інших чинників, які на них впливають;

оптимізувати процес обробки інформації для прийняття рішення з питань розподілу ОВТ і МТЗ, формування документів на їх видачу та списання, у т.ч. бойових втрат і нестач, ведення бази даних з використання і ремонту ОВТ;

деталізувати необхідні дані та формувати розрахунки для обґрунтування заходів; відпрацьовувати звіти, донесення, фінансові документи за визначеними Генеральним штабом, Міноборони, Кабінетом Міністрів формами у розрізі номенклатур служб, класів постачання, кодів груп спроможностей забезпечення (SUSTAIN) Єдиного переліку (Каталогу) спроможностей Міністерстві оборони України та ЗС України щодо руху ОВТ і МТЗ у військових частинах, у тому числі з врахуванням специфіки їх експлуатації (використання) під час виконання бойових завдань;

уточнювати потребу та розподіл ресурсів, необхідних для досягнення визначених спроможностей, або яких не вистачає для виконання визначених завдань; виявляти показники різниць між потрібними та наявними спроможностями військових частин.

Висновок. Таким чином автоматизація процесів здійснення розрахунків із логістичного забезпечення Збройних Сил повинна підвищити ефективність роботи органів військового управління, оптимізувати використання ресурсів, раціонально розподілити рух ОВТ і МТЗ, та у цілому надати командуванню пропозиції для прийняття рішень із всебічного забезпечення виконання завдань. Зазначені пропозиції стосовно напрямів автоматизації процесів здійснення розрахунків із логістичного забезпечення дадуть змогу у режимі реального часу готувати розрахунки та необхідні інформаційні матеріали за напрямками служб забезпечення у розрізі їх номенклатур, класів постачання, з врахуванням у подальшому кодів груп спроможностей забезпечення (SUSTAIN) Єдиного переліку (Каталогу) спроможностей Міністерства оборони України та Збройних Сил України щодо руху ОВТ і МТЗ під час виконання бойових завдань. Розроблені пропозиції доцільно використовувати під час подальших досліджень проблем з удосконалення підходів до порядку автоматизації процесів управління логістичним забезпеченням Збройних Сил.

ЛІТЕРАТУРА

1. Стратегічний оборонний бюлетень України, введений в дію Указом Президента України від 6 червня 2016 року № 240/2016, [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/Laws/show/240/2016.

2. Гаврилюк І.Ю. Щодо впровадження логістичної системи НАТО в Україні, Гаврилюк І.Ю., Степанюк М.Ю., Сініцин І.П., Котеля О.В., [Електронний ресурс]. – Режим доступу: http://defpol.org.ua/index.php/produkty-tsentru/aleia-heroiv/481shchodo-vprovadzhennya-lohistychnoyi-systemy-nato-v-ukrayini.

3. Закалад М.А. Підходи до автоматизації процесів логістичного забезпечення Збройних Сил України. [Текст] / Закалад М.А., Утюшев М.К., Бобров С.В. // Зб. наук. пр. Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. – 2018. – № 3(64), [Електронний ресурс]. – Режим доступу: https://nuou.org.ua/assets/journals/zbirnyk_cvsd/zb-3-64-2018.pdf

4. Люлін Д.О. Удосконалення системи технічного забезпечення засобів зв'язку і автоматизації Збройних Сил України, Люлін Д.О., Михайлов О.В., Кайдаш І.Н., Збірник наукових праць ВІТІ НТУУ „КПІ" № 2 – 2011, [Електронний ресурс]. – Режим доступу: http://www.viti.edu.ua/files/zbk/2011/zb_1102.pdf

5. Меленчук В.М. Управління проектами/програмами/портфелями впровадження інформаційних технологій в автомобільному господарстві військових формувань / Меленчук В.М., Березенський Р.В.// Управління проектами та розвиток виробництва. – 2016. – № 2. – С. 5-11. [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/UJRN/Uprv_2016_2_3.

д.т.н. Лисенко О.І. (НТУУ „КПІ”)
к.т.н. Явіся В.С. (НТУУ „КПІ”)
Петрова В.М. (НТУУ „КПІ”)

ВИБІР СПОСОБУ ОДЕРЖАННЯ КЕРУЮЧОЇ ІНФОРМАЦІЇ СИСТЕМОЮ СТАБІЛІЗАЦІЇ РУХУ НАНОСУПУТНИКІВ

Відомо, що наносупутники (НС) можуть використатися як ретрансляційна мережа, для дистанційного зондування Землі, наукових місій, екологічного моніторингу, прогнозу землетрусів, дослідження іоносфери, для розвідки та навігації.

При цьому, незалежно від призначення, а відповідно і того, яка система стабілізації й орієнтації буде використовуватися, для її роботи необхідно одержати сигнали управління. Таке завдання вирішується як правило за допомогою інерційних систем [1].

При русі НС у полі тяжіння вимірюване акселерометром прискорення відрізняється від дійсного й тому одержало назву гаданого прискорення. Його вимір дозволяє визначити дійсне положення НС щодо центру тяжіння.

Для управління необхідно знати три ортогональні складові вектора гаданого прискорення центру маси НС, тобто мати три датчики, встановлені у центрі маси НС, із трьома взаємно перпендикулярними осями чутливості [2].

Технічна реалізація методу інерційного управління можлива у двох варіантах. Перший – за допомогою пристроїв, які не обертаються разом із НС і, зберігаючи своє положення відносно інерційного базису, служать опорою для вимірювальної системи. Другий варіант − за допомогою пристроїв, які забезпечують обчислення параметрів, що визначають кути між осями вимірювальної системи й інерційного базису, а також проектування вимірюваних компонентів прискорення на осі цього базису.

Перший варіант вимагає наявності приладів, що фізично моделюють інерційний базис на борті НС, − гіростабілізованих платформ, другий − використання безплатформових систем.

При реалізації платформових систем забезпечення необхідної надійності й збільшення точності виявилось пов’язаним зі значним ростом маси й габаритів платформ, негативною є і їх чутливість до великих перевантажень і кутів обертання, що характерно для НС. Тому безплатформні інерційні системи (БІС), завдяки наявності сьогодні високошвидкісних обчислювальних пристроїв у мініатюрному виконанні, займають лідируюче положення при створенні нових систем управління об'єктами, для яких є критичними ваго-габаритні показники таких систем [2, 3].

У безплатформних системах стабілізації (БСС) зв'язок між інерційним і вимірювальним базисами виражається в процесі обчислень через параметри, які не можуть безпосередньо служити параметрами управління. Рівняння руху НС повинні бути записані через вимірювані датчиками параметри й через параметри зв'язку в реальному часі. В цілому розробку БСС доцільно будувати таким чином, щоб визначити метод, що дозволяє одержати сигнали управління, які забезпечують роботу виконавчих органів систем орієнтації й стабілізації положенням НС [2].

Первинна інформація про параметри кутового руху НС може бути отримана у вигляді прискорення крапки установки вимірювального приладу або інтегралів цього прискорення. Варіанти побудови БСС залежно від співвідношення величин, які безпосередньо вимірюються й обчислюються, можна розбити на три підкласи [2]: системи, де вимірюються тільки лінійні прискорення, а всі інші параметри обчислюються; системи, де вимірюються, крім лінійних параметрів, і кутові швидкості; системи, де вимірюються будь-які параметри, включаючи й кути Ейлера.

Система на основі датчиків лінійних прискорень. Для того щоб обчислити параметри кутового положення НС, необхідно знати його кутову швидкість відносно інерційного базису.

Для вимірювання кутової швидкості використовуються акселерометри з інтегральним виходом. Максимально можлива на сьогодні точність зазначених приладів виявляється такою, що помилка обчислень уже за 2-3 хвилини накопичується до величин, порівнянних з вимірюваними значеннями, тому система на основі одних датчиків лінійних прискорень поки представляє лише теоретичний інтерес [4].

Система з виміром лінійних прискорень і кутової швидкості. Усі існуючі й перспективні високоточні датчики лінійних прискорень і кутових швидкостей дозволяють одержувати інформацію тільки у вигляді приросту інтегралів від названих параметрів, тобто, по суті, є датчиками приросту лінійної швидкості й кутів обертання НС. Але такі параметри, як лінійне прискорення й кутова швидкість, мають набагато більш глибокий фізичний зміст, ніж приріст їх інтегралів. Тому в цьому випадку можна говорити про існування двох методів:

- будувати математичний апарат паралельно для безпосередньої й інтегральної форми знімання інформації з вимірювальної системи;
- при розв'язку теоретичних питань вважати, що інформація про параметри руху доступна в дійсній розмірності останніх, а практично інтегральний її характер ураховується при розробці конкретних алгоритмів побудови ІКБ.

Для обчислення параметрів руху НС необхідно знати вектор прискорення його центру маси й вектор кутової швидкості обертання біля центру маси. Таким чином, вимірювальна система повинна мати, мінімум три датчики лінійних прискорень і три датчики кутової швидкості.

Система на основі датчиків, що вимірюють кути Ейлера. Відлік кутів Ейлера проводиться від інерційного базису, тому його фізичне моделювання є неминучим. Однак у цьому випадку на відміну від звичайних платформних систем моделюються тільки вимірювальні осі, а не платформа для розміщення датчиків лінійних прискорень. Таким чином, для одержання інерційних компонентів вектора швидкості необхідно вимірювання, які здійснюються відносно зв'язаної системи координат, перераховувати до інерційного координатного базису (ІКБ).

Перевагою подібної системи є економія обчислювальних ресурсів при аналітичній побудові інерційного базису. Значним недоліком є обмеження максимальних кутів повороту й припустимих перевантажень через наявність вільних гіроскопічних систем на борті НС. Система з виміром кутів Ейлера може розглядатися як граничний випадок між платформним і безплатформним варіантами: по наявності фізичних моделей ІКБ на борті цю систему можна віднести до категорії звичайних інерційних, а по характеру розташування датчиків прискорення − до категорії безплатформних систем. Відзначений недолік системи з вільними гіроскопічними приладами зводить до мінімуму переваги БІС.

Тому при побудови системи стабілізації НС для одержання керуючої інформації доцільно використовувати системи з виміром лінійних прискорень і кутової швидкості.

ЛІТЕРАТУРА

1. Явися В.С. Способы управления пространственным положением наноспутника // Десята міжнародна науково-технічна конференція «Проблеми телекомунікацій». Збірник тез. – К.: НТУУ „КПІ”. – 2016. – С. 507 – 510.

2. Лебедев Р. К. Стабилизация летательного аппарата бесплатформенной инерциальной системой. – М.: Машиностроение, 1977. − 144 с.

3. Гущин В.Н. Основы устройства космических аппаратов. – М.: Машиностроение, 2003 г. – 272 с.

4. Литвин М.А., Малюгина А.А., Миллер А.Б. Типы ошибок в инерциальных навигационных системах и методы их аппроксимации // Информационные процессы. – 2014. − Том 14. − № 4. − С. 326 – 339.

д.т.н. Лисенко О.І. (НТУУ „КПІ”)
к.т.н. Явіся В.С. (НТУУ „КПІ”)
Явіся Д.В. (НТУУ „КПІ”)

СИСТЕМА ОРІЄНТАЦІЇ ТЕЛЕКОМУНІКАЦІЙНИХ НАНОСУПУТНИКІВ

За останні роки завдяки мініатюризації електронних компонентів відбувається стрімкий розвиток нового виду космічної техніки – наносупутників (НС). Сфера їх застосування в перспективі виявляється навіть ширше, ніж звичайних супутникових платформ. Ряд застосувань НС можливий тільки у випадку рішення завдання забезпечення стабільного та керованого положення НС на орбіті.

Завдання орієнтації й стабілізації вирішується двома методами [1]: пасивним та активним. Система орієнтації телекомунікаційного НС повинна будуватись на активних методах, оскільки лише вони, окрім стабілізації, здатні забезпечити оперативну зміну орієнтації всього НС або його зовнішніх конструктивних елементів. Активні методи стабілізації реалізують за допомогою двигунів-маховиків, моментного магнітопривіду або реактивних двигунів (РД). Причому РД вимагають наявності на борту значних запасів палива, тому, останнім часом широко застосовують іонні двигуни (ІД), для роботи яких необхідна на порядок менша кількість палива, ніж для звичайних РД.

Для оцінки ефективності активних методів орієнтації зробимо ряд уточнень. НС стандарту CubeSat являє собою куб з ребром $R = 0{,}1$ м та масою близько $m_{нс} = 3$ кг. При використанні двигунів-маховиків на одній осі розташовується два маховики, які працюватимуть синхронно. При реалізації моментного магнітопривіду для орієнтації по одній осі необхідне застосування двох котушок, розташованих під прямим кутом одна відносно іншої. ІД розташовуються на краю поверхні певних сторін CubeSat. Оскільки, для системи на двигунах-маховиках зміна швидкості обертання маховиків відбувається майже миттєво, при розрахунках цей час можна не враховувати. У свою чергу робота систем з моментним магнітопривідом та з ІД фактично відбувається в два однакові за тривалістю етапи – на першому відбувається розгін до певної кутової швидкості обертання, а на другому – гальмування [2].

Тоді, можна показати, що кут повороту НС навколо певної осі для різних систем орієнтації визначають наступні вирази:

- для системи на двигунах-маховиках:

$$\alpha_{нс}(t) = 3\frac{m_м r^2}{m_{нс} R^2}\omega_м t \tag{1}$$

де $m_м$ – маса маховика; r – радіус диска маховика; $\omega_м$ – швидкість обертання маховика;

- для системи з моментним магнітопривідом:

$$\alpha_{нс}(t) = \frac{3IpSB}{2m_{нс} R^2}t^2 \tag{2}$$

де I – струм котушки; p – число витків котушки; S – площа рамки котушки; B – індукція магнітного поля Землі;

- для системи з ІД:

$$\alpha_{нс}(t) = \frac{3F}{4m_{нс} R}t^2 \tag{3}$$

де F – сила, що розвивається ІД.

Зазначимо, що для системи на двигунах-маховиках кут обертання є лінійною функцією часу, а для систем з моментним магнітопривідом та з ІД – залежність квадратична. Для порівняння активних систем були обрані наступні значення параметрів, що входять до

формул (1-3): $m_м = 0{,}02$ кг, $r = 0{,}03$ м, $\omega_м = 1{,}16$ рад/с (в середньому 4000 обертів за хвилину), $I = 0{,}43$ А, $p = 100$, $S = 0{,}005$ м^2, $B = 30$ мкТл, $F = 100$ мкН.

Часова залежність величини кута повороту для певної системи із урахуванням зазначених вище допущень представлена на рис. 1, відповідно до якого можна заключити, що всі три системи володіють приблизно однаковими можливостями на інтервалі часу до 15 с, впродовж якого кутове положення НС змінюється майже на 0,7 рад або 4 градуси. Причому добір параметрів та аналіз проведений за умови, що системи мають близькі ваго-габаритні характеристики та показники енергоспоживання. Повний оберт навколо певної вісі відбудеться менш ніж за дві хвилини. Зазвичай такої швидкодії системи орієнтації для телекомунікаційного НС цілком достатньо. Але кожна із систем має певні недоліки: системи на двигунах-маховиках потребують періодично здійснювати їх розвантаження; системи із моментним магнітопривідом не забезпечують одночасну тривісну орієнтацію, що пов'язано із структурою магнітного поля Землі; системи з ІД мають ресурс роботи, який обмежений запасами палива.

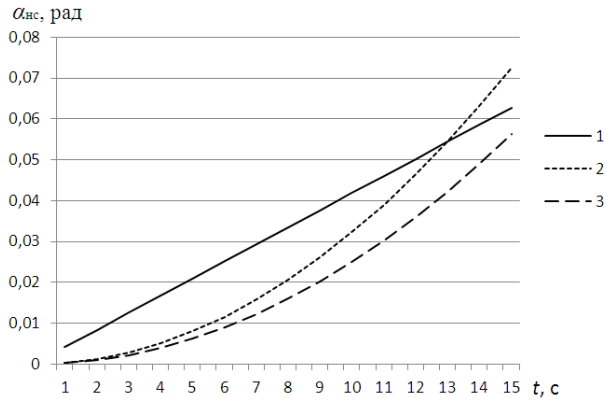


Рис . 1. Часова залежність величини кута повороту НС: 1 – для системи на двигунах-маховиках, 2 – для системи із моментним магнітопривідом, 3 – для системи з ІД.

З погляду на це обґрунтованим буде одночасне використання хоча б двох систем. Однак зазначимо, що лише компактні іонні прискорювачі дозволять НС змінювати орбітальну позицію або утримуватись на ній тривалий час. Також двигуни малої тяги можуть використатися для керованого сходу з орбіти ушкоджених НС. Це змусить їх згоряти в атмосфері Землі й частково вирішить проблему космічного сміття. Оскільки системи орієнтації на двигунах-маховиках та магнітних виконавчих органах не дозволяють здійснювати зміни орбіти НС, найбільш доцільним буде використання комбінованої системи, яка може бути реалізована в двох варіантах. В першому, вона складається з двигунів-маховиків та ІД, в другому – з магнітних котушок та ІД. Двигуни-маховики або магнітні котушки дозволяють вирішувати завдання стабілізації й орієнтації. ІД в першому варіанті реалізації будуть задіяні, в основному, для періодичного розвантаження двигунів-маховиків, в другому – для допомоги системі з моментним магнітопривідом виконувати одночасну тривісну орієнтацію. Але в обох варіантах ІД забезпечать можливість зміни орбіти НС, що в цілому дозволить значно збільшити їхній термін служби, а також здійснювати плановий відхід з орбіти по закінченні експлуатації.

ЛІТЕРАТУРА

1. Левантовский В. И. Механика космического полета в элементарном изложении. – М.: Наука, 1980. 512 с.

2. Явися В.С., Лысенко А.И. Анализ методов ориентации и стабилизации наноспутника // Науковий вісник Академії Муніципального Управління, Збірник наук. праць АМУ. Серія „Техніка". – Вип.1-2(11)–2016. – К.: АМУ, 2016. – С. 262 – 270.

к.т.н. Лівенцев С. П. (ІСЗЗІ НТУУ „КПІ”)
к.т.н. Павлов В. П. (ІСЗЗІ НТУУ „КПІ”)
к.т.н. Василюк Ю. С. (ІСЗЗІ НТУУ „КПІ”)
Ляшенко Г.Т. (ВІТІ)

АЛГОРИТМ СЛІПОЇ ОБРОБКИ ОЦІНЮВАННЯ СКАЛЯРНИХ ТА ВЕКТОРНИХ КАНАЛІВ ПРИ ДЕКОДУВАННІ ТУРБОКОДІВ В КАНАЛАХ З СТРУКТУРНИМИ ЗАВАДАМИ

Постановка задачі. Завдання підвищення достовірності прийняття рішень по надійності декодування символів (біт) в турбокодах (ТК) вирішується шляхом ідентифікації та оцінювання каналу. У скалярному каналі, тобто в каналі з одним входом і виходом, алгоритми сліпої ідентифікації (СІ), як правило, вимагають деякої статистичної вибірки інформаційних блоків на виході каналу для побудови оцінки.

Сліпа обробка (*blind signal processing*) – це технологія цифрової обробки сигналів, яка отримала свій розвиток протягом останніх років. У загальному вигляді завдання сліпої обробки можна сформулювати як цифрову обробку невідомих сигналів, що пройшли лінійний канал з невідомими характеристиками на фоні адитивних шумів.

Мета. Розробка алгоритму сліпої обробки оцінювання скалярних та векторних каналів (СК та ВК) при декодуванні ТК в каналах зі структурними завадами

Актуальність. У загальному випадку для стаціонарного гауссовського каналу повна ідентифікація неможлива. Якісно, без прив’язки до конкретного методу ідентифікації і властивостей каналу, для отримання сліпої оцінки в СК потрібна інформаційна послідовність, довжина якої зазвичай на 2 порядки перевищує довжину каналу. При цьому якість оцінки наближається до оцінки за тестовим сигналом. Тому виникає протиріччя між складністю оцінювання каналу та часом обробки послідовності.

Основні положення. Використання статистик 2-го порядку для СІ СК можливе в цілому для нестаціонарної моделі вхідного сигналу і в частковому випадку періодично-корельованого (циклостаціонарного) сигналу.

Використовуючи поліноміальні статистики, розв’язок задачі СІ зводиться до задачі розв’язання систем поліноміальних рівнянь від багатьох змінних. Даний підхід є узагальненням підходу, що заснований на використанні поліспектрів (методи статистик високого порядку), відомих в теорії зв’язку. Даний підхід може бути узагальнений і на випадок ВК.

Модель ВК використовується для опису рознесеного прийому (в просторі або в часі). Умови ідентифікації ВК сформульовані в рамках детермінованої моделі, тобто СІ здійснюється по одній реалізації, також як і при використанні тестового сигналу. При цьому співвідношення довжин каналу та інформаційної послідовності становить приблизно один порядок, що дозволяє використовувати ці технології в каналах з швидкими завмираннями.

Можливість статистичної СІ каналу за моментними функціями випадкового процесу 2-го порядку на виході каналу забезпечується наданням в загальному випадку стаціонарному інформаційному сигналу додаткових нестаціонарних властивостей, що сприяють подальшій СІ. При цьому модель періодично корельованого процесу на вході є окремим випадком для загальної нестаціонарної моделі просторово-часового каналу.

Висновок. При застосуванні методу СІ оцінка імпульсної характеристики може далі використовуватися для оцінки інформаційної послідовності, тобто є першим етапом сліпого вирівнювання, яке може бути використане для підвищення достовірності прийняття рішення під час декодування ТК. Запропоновано підхід до синтезу алгоритмів СІ на основі поліноміальних статистик, який дозволяє за єдиним алгоритмом синтезувати різні методи СІ для скалярних каналів зі стаціонарним і нестаціонарним входом, різних розподілів вхідних символів. На відміну від підходу на основі поліспектрів, в даному випадку може бути знижена невизначеність вибору набору кумулянтних функцій в процедурі синтезу алгоритму.

к.т.н. Ліщинська Х.І. (НАСВ)
к.т.н. Сокіл М.Б. (НУЛП)
к.ф.-м.н. Сокульська Н.Б. (НАСВ)
к.ф.-м.н. Сеник А.П. (НУЛП)

ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНИХ СИСТЕМ З ВИКОРИСТАННЯМ СПЕЦІАЛІЗОВАНИХ МАТЕМАТИЧНИХ МЕТОДІВ

Актуальність. Великі обсяги даних, які можна належним чином систематизувати, є актуальною перевагою для багатьох галузей, включаючи військову. Неможливо здійснювати ефективні військові дії, не маючи якнайповнішої інформації щодо наявних ресурсів. Великі військові набори даних допомагають штабам приймати вірні рішення за умови, що їх можна певним чином опрацювати. Термін „великі дані" було введено більше як два десятиліття тому в документі, представленому на 8-ій конференції IEEE з питань візуалізації. Цей термін характеризує настільки великі набори даних, що вони не вписуються в основну пам'ять. Якщо говорити про сьогодення, то обсяг світових даних у 2013 році становив 4,4 зетабайт і інтенсивно зростає й надалі. Крім того, останні розробки в галузі штучного інтелекту та технологій машинного навчання також значно збільшують процес накопичення даних.

Пошук нової інформації з масиву оперативних даних можливий лише за умови їх аналізу у єдиному форматі. Великий обсяг накопичених даних може зробити цей процес нездійсненим для спеціалістів, що користуються звичайними методами їх опрацювання. Складність полягає в тому, що ці дані перетворюються на нагромадження інформації без жодної користі, навіть якщо відомо, що серед них є такі, які мають великий інформаційний потенціал. Більшість завдань з пошуку даних за певною класифікацією та при об'єднанні їх правил відбору страждають від накладених обмежень у практичному застосуванні, зокрема і через ітеративний характер алгоритмів обробки, пов'язаний з великою кількістю доступних даних, що обмежується апаратними платформами для їх обробки.

Мета. Впровадження методу Data Discovery для швидкого опрацювання великих інформаційних потоків як один зі шляхів прийняття оптимальних військових рішень.

Основні положення. Інструмент роботи з великими обсягами даних різного походження Data Discovery допомагає використовувати зібрані дані для виявлення нових закономірностей та можливостей. Це спричиняє знаходження оптимальних стратегій і тактичних ходів, ефективних операцій, якісних високих результатів, а також отримання переваг у різних напрямах діяльності, зокрема військової. Тому створення прикладного програмного забезпечення, яке, використовуючи метод Data Discovery, здійснює аналіз конкретних даних, залишається актуальним.

Метод Data Discovery дозволяє розширити основні компетенції користувачів та відповідає новим вимогам для швидкості аналізу та управління великими наборами даних. Зокрема цей метод дозволяє організувати сховище даних. Він виконує проміжні операції, такі як оптимізація і аналітика, що є важливими для роботи інформаційної платформи, але значною мірою невидимі для кінцевого користувача, а також дозволяє організувати повний набір інструментів для виявлення закономірностей у даних, і є орієнтований на надання інформації, прийняття обґрунтованих рішень і виявлення нових тактичних можливостей. У простих термінах, метод Data Discovery є процесом пошуку закономірностей у даних і їх використання для досягнення конкретних, в тому числі й військових, цілей.

Висновки. Таким чином, запропонований до розгляду спеціалізований математичний інструмент Data Discovery з використанням методів інтелектуального та оперативного аналізу даних, дозволяє збільшити якість аналітичної обробки даних, зокрема військового характеру, які мають різні джерела походження, вдосконалити управлінську функцію і може застосовуватись в експертних системах, а також в системах прийняття рішень. Крім того, Data Discovery використовується при організації автономних інформаційних систем, здатних до самонавчання.

к.т.н. Мазулевський О.Є. (ВІТІ)
Саченко А.П. (ВІТІ)
Толстих В.А. (ВІТІ)

АНАЛІЗ МОЖЛИВОСТЕЙ IPS РІВНЯ МЕРЕЖІ

Перебіг останніх збройних та військових конфліктів показав важливість використання мережних технологій та використання їх вразливостей у противника. Тому державами почали вивчатися і одночасно застосовуватися методи роботи мережних зловмисників – хакерів. Для реалізації впливу на протилежну сторону почали застосовуватися елементи атак в кібернетичному просторі. Вивчення об'єкту атаки найважливіший етап її здійснення. Від того на скільки якісно буде вивчено об'єкт на стільки вдалою і буде атака. З часом методи дії хакерів почали використовуватися і в процесі захисту мережної інфраструктури з метою виявлення „уразливостей" в захисті систем. У даний час проведення сканування безпеки допомагає компаніям знайти уразливості, які можуть бути використані хакерами.

Зараз існує цілий клас програмного забезпечення такого як „сканери безпеки" (СБ). Вони дозволяють отримати досить докладне й актуальне уявлення про поточний стан інформаційної безпеки системи. Мінімум, що надають такі СБ - це можливість, для оцінки поточного рівня захищеності, а більш досконалі версії можуть надавати інструменти для усунення виявлених вразливостей. Застосування СБ є актуальним питанням в побудові та експлуатації інформаційно-телекомунікаційних мереж в ЗС України. Метою доповіді є порушення питання порівняння декількох систем виявлення вразливостей для визначення раціонального варіанту використання в Збройних Сил України. Перші програмні реалізації СБ або систем виявлення вторгнень, були ще в 90-х роках XX століття. Одним з перших мережних сканерів був SATAN – System Administrator Tool for Analysis of the Network. В часи появи цього програмного забезпечення ситуація з безпекою в Інтернет була катастрофічною. Тому поява SATAN – засобу, доступного для використання усіма зацікавленими користувачами, спричинила великий розголос. Навіть були спроби заборонити розробку і розповсюдження подібних засобів через погану захищеність вузлів мережі, але суспільство зрозуміло, що слід підтримувати достатній рівень захищеності вузлів мережі і для їх контролю періодично застосовувати СБ. Тому на сьогоднішній час існує велика кількість праць з дослідження різних методів та способів роботи СБ, їх переваг та недоліків.

Зокрема в них визначено, що сканери вразливості діляться на дві основні групи:

- активні СБ, призначені для аналізу мережі, ОС та додатків на наявність уразливостей;
- пасивні СБ, які спостерігаючи за мережним трафіком шукають можливі уразливості.

СБ мають багато можливостей та засобів для ефективного виявлення і управління виправленнями вразливостей, які виявлені після аналізу та фільтрації результатів. Функціонувати такі засоби можуть на мережному рівні, рівні операційної системи і рівні додатку. Найбільшого поширення набули засоби аналізу захищеності мережних сервісів і протоколів. Пов'язано це, в першу чергу, з універсальністю використовуваних протоколів. Вивченість і повсюдне використання стандартизованих протоколів різних рівнів дозволяють з високим ступенем ефективності перевіряти захищеність системи, що працює в даному мережному оточенні. Другими за поширеністю є засоби аналізу захищеності операційних систем. Пов'язано це також з універсальністю і поширеністю різних операційних систем.

Захист мережі від несанкціонованих дій являє собою найважливішу задачу для всіх організацій різного рівня. Щоб попередити і виключити спроби злому, зміни чи видалення інформації використовуються різні засоби для захисту своєї мережі. Одними з обов'язкових для використання вважаються СБ, призначення яких полягає в здійсненні діагностики і моніторингу мережних комп'ютерів, що дозволяє сканувати мережі, комп'ютери та програми на предмет виявлення можливих проблем у системі безпеки, оцінювати і усувати вразливості. Кожен зі СБ має свої переваги та свої недоліки, тому вибір зазвичай ґрунтується на можливостях організації та її взаємодії зі СБ.

к.т.н. Макарчук І.М.(ВІТІ)
Скиба С.Є.(ВІТІ)

ІНФОРМАЦІЙНА СИСТЕМА АВТОМАТИЗАЦІЇ ПРОЦЕСІВ РОБОТИ НАУКОВО-ТЕХНІЧНОЇ БІБЛІОТЕКИ ВВНЗ В РАМКАХ КОХА

Постійне збільшення об'ємів інформації в усіх сферах діяльності людини, а також складність та об'єм неавтоматизованої обробки документів стимулюють застосування комп'ютерів і пов'язаних з ними засобів та технологій у практику бібліотечно-інформаційної роботи.

Автоматизація привносить в роботу бібліотеки цілий ряд нових можливостей, одночасно усуваючи значну кількість рутинних операцій, а отже – і підвищує ефективність роботи.

Мета автоматизації робочих процесів – це перш за все: підвищення продуктивності та ефективності праці співробітників бібліотеки і, як результат, – якісно виконана бібліотечна послуга.

Проаналізувавши предметну область вирішили взяти за основу автоматичну бібліотечну інформаційну систему КОХА.

КОХА має більшість очікуваних можливостей програмного забезпечення автоматизованих бібліотечних інформаційних систем, зокрема:

–Простий, зручний інтерфейс для бібліотекарів та читачів (відвідувачів)

–Пошук, що гнучко налаштовується

–Обіг та керування позичальниками

–Модуль каталогізації з вбудованим клієнтом Z39.50/SRU

–Повна система надходжень, зокрема бюджетні витрати та цінові дані (з включенням постачальників та конверсією валют)

–Проста система надходжень для маленької бібліотеки

–Здатність працювати з будь-якою кількістю підрозділів, відвідувачів, категорій відвідувачів, примірників, категорій примірників, валют та інших даних

–Система періодики для журналів або ж газет

–Списки прочитаного для відвідувачів

Серверна сторона автоматичної бібліотечної інформаційної системи КОХА написана на мові програмування *Perl* і вимагає:

–*Perl*

–Веб-сервер *Apache* (2.0 вважається кращою)

–Сервер *MySQL 5* (починаючи з 4.1 належно обробляється кодування)

–Модулі *Perl* для деяких функцій

Perl (*Practical Extraction and Reporting Language* — практична мова витягів та звітів) — високорівнева, інтерпретована, динамічна мова програмування загального призначення.

Клієнтська частина інтерфейсу (електронний каталог) АБІС КОХА написана на *XHTML* з використанням *CSS 2.0*, використовує графіку *PNG* та правильно відображатиметься у будь-якій операційній системі у будь-якому, сумісному з *CSS 2.0*, браузері.

Інтерфейс бібліотекарів має подібні вимоги, але вимагає правильної роботи броузера з *Javascript.*

Детально розглянувши можливі даної автоматичної бібліотечної інформаційної системи було вирішино, що потрібно привести в КОХА ряд покращень щоб вона могла задовольняти в повній мірі потреби ВВНЗ. Тому було вирішено створити власну бібліотеку для АБІС КОХА яка б принесла бажані покращення.

Макарчук В.І. (ВІТІ)
Мартинюк В.В. (ВІТІ)
Паламарчук С.А. (ВІТІ)
Карпенко А.О. (ВІТІ)

ПОРІВНЯННЯ ЗМІСТУ І ПОСЛІДОВНОСТІ РОБОТИ ПРИ ПЛАНУВАННІ ЗВ'ЯЗКУ В ОРГАНАХ ВІЙСЬКОВОГО УПРАВЛІННЯ ОПЕРАТИВНОГО РІВНЯ ЗГІДНО КЕРІВНИХ ДОКУМЕНТІВ ЗБРОЙНИХ СИЛАХ УКРАЇНИ ТА ЗГІДНО СТАНДАРТІВ НАТО

Актуальність Міністерство оборони України продовжує процес запровадження стандартів і критеріїв Збройних сил провідних країн світу в діяльність Збройних сил України у відповідності до положень Тимчасової інструкції з організації робіт у Міністерстві оборони України та Збройних силах України щодо впровадження стандартів НАТО. Цей документ визначає організаційні питання прийняття та впровадження положень, норм і вимог НАТО у Збройних силах України з метою досягнення їхньої сумісності з арміями країн-партнерів, підвищення ефективності системи управління. Тому і постає необхідність провести порівняння змісту і послідовності роботи при плануванні зв'язку згідно керівних документів Збройних Сил України та згідно стандартів НАТО.

Основні положення. Зв'язок в органах військового управління (далі – ОВУ) Збройних сил України планується у відповідності до положень Тимчасової настанови з організації зв'язку та інформаційних систем та керівництв, положень, інструкцій тощо, які встановлюють порядок виконання завдань щодо: організації радіорелейних і тропосферних ліній зв'язку, оперативно – технічної служби на вузлах зв'язку, безпеки застосування зв'язку та інших. Зв'язок в органах військового управління об'єднаних збройних сил НАТО планується у відповідності до положень: союзницької публікації НАТО AJP-01 „Єдина доктрина спільних дій", союзницької публікації НАТО AJP-3 „Доктрина спільних дій при проведенні операцій", союзницької публікації НАТО AJP-6 „Єдина доктрина для систем зв'язку та інформаційних систем" та інших документів, які стосуються організації зв'язку та в даний час знаходяться на стадії перекладу та досліджень.

Робота начальника управління зв'язку при плануванні зв'язку в ОВУ ЗС України включає три послідовних та взаємопов'язаних етапи:

організація планування зв'язку;

вироблення замислу організації зв'язку;

розроблення плану зв'язку.

Робота начальника управління J-6 об'єднаних збройних сил (далі – ОЗС) НАТО при плануванні зв'язку в ОВУ включає вісім послідовних та взаємопов'язаних кроків:

I крок: (початковий) – Ініціювання прийняття та опрацювання рішення старшим штабом (командиром).

II крок: Оцінка обстановки та аналіз місії.

III крок: Розробка курсу діяльності.

IV крок: Аналіз курсу діяльності.

V крок : Перевірка та порівняння курсу діяльності.

VI крок : Рішення начальника J-6 щодо курсу діяльності.

VII крок: Розроблення плану забезпечення системи зв'язку та інформаційної системи (далі – СЗІС).

VIII крок: Проведення оцінки перегляд/ коригування плану забезпечення СЗІС.

Процес планування зв'язку в ОВУ закінчується затвердженням та доведенням до підпорядкованих військ планувальних та директивних документів зі зв'язку, а саме:

– в ОВУ ЗС України: розпорядження зі зв'язку підпорядкованим штабам військових частин (підрозділів), плану зв'язку ОВУ, бойового розпорядження підпорядкованій військовій частині зв'язку;

– в ОВУ ОЗС НАТО: план забезпечення СЗІС, план управління спектром бойового простору, параграф 5 „Організація управління та зв'язку" бойового наказу командувача ОВУ об'єднаних збройних сил НАТО.

Перший етап „Організація планування зв'язку" процесу планування зв'язку в ОВУ ЗС України містить наступні процедури: аналіз завдання, оцінювання обстановки та формування вихідних даних для планування зв'язку співпадає з кроками: I „Ініціювання прийняття та опрацювання рішення старшим штабом (командиром)" та II „Оцінка обстановки та аналіз місії", які проводять при плануванні зв'язку в управлінні J-6.

Наприкінці цих етапів та кроків здійснюється первинна оцінка, узагальнюються висновки, проводиться розрахунок необхідного часу на планування та віддаються попередні розпорядження підпорядкованим частинам.

Під час другого етапу „Вироблення замислу організації зв'язку" в ОВУ ЗС України начальником управління зв'язку визначається найбільш доцільний варіант організації зв'язку відповідно до обраного способу проведення операції та здійснюється прийняття рішення на організацію зв'язку, в якому визначаються:

порядок організації управління;

завдання підпорядкованим штабам та військовим частинам;

порядок організації управління зв'язком;

основні питання взаємодії між військовими частинами (підрозділами) зв'язку;

основні завдання за видами забезпечення.

Цьому етапу планування за змістом відповідають: кроки III „Розробка курсу діяльності" та VI „Рішення начальника J-6 щодо курсу діяльності" процесу планування зв'язку в ОВУ ОЗС НАТО під час яких здійснюється аналіз відносної боєздатності (спроможностей) наявних сил та засобів зв'язку, розробляються варіанти порядку виконання завдань та приймається рішення щодо остаточного варіанту організації зв'язку.

На третьому етапі „Розроблення плану зв'язку" начальник управління зв'язку ОВУ ЗС України здійснює:

розроблення плану зв'язку;

розгляд та затвердження документів плану зв'язку.

Після цього здійснюється аналіз та оцінювання документів плану зв'язку та розробка нових документів у разі необхідності. Даному етапу відповідають кроки VII „Розроблення плану забезпечення СЗІС" та VIII „Проведення оцінки (перегляд та коригування) плану забезпечення СЗІС" на яких начальник управління J-6 здійснює аналогічні заходи щодо розроблення, затвердження, аналізу, коригування та розробки нових документів плану забезпечення системи зв'язку та інформаційних систем у разі необхідності. На цих же кроках управлінням J-6 розробляється план управління спектром бойового простору.

Висновок. Процес планування зв'язку в ОВУ ЗС України визначений в керівних документах ЗС України має спільні риси з процесом планування зв'язку в ОВУ ОЗС НАТО, який здійснюється у відповідності до положень стандартів НАТО. Важливо звернути увагу на відмінності в підходах щодо планування зв'язку, а саме: управління J-6 штабу ОВУ ОЗС НАТО спочатку планує сервіси якими необхідно забезпечити підпорядковані частини для проведення операції, після цього приступає до побудови СЗІС. Це дозволяє економно витрачати ресурси зв'язку (не здійснювати розгортання в операційних районах надлишкових засобів зв'язку). В ЗС України управління зв'язку штабу ОУВ спочатку планує систему зв'язку та інформаційні системи та дає розпорядження на їх розгортання у повному обсязі, а далі визначається з сервісами, якими необхідно забезпечити підпорядковані військові частини (підрозділи) для проведення операції (бойових дій). В даному випадку система зв'язку має більшу стійкість, але витрачається ресурс сил та засобів зв'язку, які на початковому етапі не приймають участь (можливо і не будуть приймати) в забезпеченні зв'язком операції (бойових дій).

к.т.н. Маковейчук О.М. (ХНУРЕ)
д.т.н. Рубан І.В. (ХНУРЕ)
д.т.н. Худов Г.В. (ХНУПС)

НОВИЙ ТИП МАРКЕРІВ ДОПОВНЕНОЇ РЕАЛЬНОСТІ

В роботі проаналізовано основні галузі застосування систем доповненої реальності. Згідно прогнозів щодо розвитку ринку AR/VR до 2025-го року за обсягом оборотів і прибутку ринок буде поділений на такі сегменти (в порядку спадання): ігри, медицина, освіта, військове застосування, виробництво і транспорт, кіно і телебачення, онлайн-трансляції, підготовка та навчання співробітників, маркетинг і реклама, роздріб/онлайн-комерція, торгівля нерухомістю. Встановлено, що в переважній більшості випадків будуть використовуватися маркерні системи доповненої реальності. Технологія систем доповненої реальності, що базується на маркерах, використовує камеру та спеціальні пасивні візуальні маркери, наприклад QR-код. Детектуючи маркери у відео-потоці, вдається вирізнити віртуальні об'єкти з реального світу. При цьому суттєвим є визначення положення камери, яке визначається засобами комп'ютерного бачення. Існуючі маркери мають певні недоліки та не завжди за допомогою їх можна вирішити нові завдання. Тому, актуальним є пошук нових маркерів доповненої реальності. В роботі запропоновано новий тип маркерів доповненої реальності, що мають переваги більшості існуючих типів маркерів та вільні від їх недоліків.

Сформульовано основні вимоги до перспективного AR-маркера:

1) легко і швидко знаходиться у відео-потоці;

2) використовується мінімальна кількість кольорів, ще краще – градації сірого;

3) містить додаткову інформацію (повідомлення);

4) дозволяє визначати положення камери;

5) пункти 3 і 4 виконуються при втраті до 50% інформації про маркер (наприклад, при закритті його завадою чи фізичній відсутності будь-якої частини маркера).

Встановлено, що жоден стандартний тип AR-маркера не буде відповідати вимогам 1–5 в повній мірі. Найближчим відповідником є 2D штрих-кодові маркери (barcode markers), але вони не задовольняють вимогам робастності 5.

У якості маркеру в роботі запропоновано використовувати QR-код як зображення-повідомлення. Він містить тільки 2 кольори і кодує в собі повідомлення. Далі пропонується наступне:

– кожен піксель зображення-повідомлення збільшуємо в k разів (тобто замінюємо матрицею k×k);

– пікселі в отриманому зображенні переставляємо псевдо-випадковим чином;

– створюємо зображення-контейнер, що складається з клітинок, кожна з яких має колір пермутованого зображення;

– для полегшення детектування цього зображення і розділення клітинок збільшимо кожну клітинку і вставимо в рамку з проміжним кольором – сірим; таким чином пропонується використовувати всього 3 кольори (градації сірого).

Показано, що запропонований маркер задовольняє всім вимогам. Теоретично обґрунтовано точність розпізнавання AR-маркера в залежності від співвідношення між його параметрами. Знайдено мінімальне значення параметра k=3 таке, що забезпечується умова робастності. Напрямками подальших досліджень є:

1) розробка методу визначення параметрів проективного перетворення, що необхідно для вирівнювання зображення і визначення положення камери;

2) розробка методу знаходження правильного зміщення вирівняного зображення у матриці N×N, що необхідно для правильного декодування пермутованого зображення.

к.т.н. Марилів О.О. (ВДА імені Є. Березняка)
к.т.н. Мєшков С.І. (ВДА імені Є. Березняка)

ПРОГНОЗУВАННЯ ІНТЕРВАЛІВ ЧАСУ ДОБИ ДЛЯ ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ, ОБЛАДНАНИХ ТЕПЛОВІЗІЙНИМИ СИСТЕМАМИ СПОСТЕРЕЖЕННЯ

Виявлення військової техніки незаконних збройних формувань (НЗФ) в темний час доби в зоні проведення операції Об'єднаних сил відбувається із використанням безпілотних літальних апаратів (БПЛА), що обладнані тепловізійними системами спостереження (ТСС). Проте проведення тепловізійного спостереження в нічний час доби супроводжується рядом труднощів. Дані труднощі викликані впливом циклічних теплообмінних процесів в навколишньому середовищі, що призводить до зміни теплової картина місцевості, а відтак, і зміни ефективності застосування ТСС. Порівняльний аналіз результатів експериментальних досліджень компанії „CMC Electronics Cincinnati" свідчить про те, що у темний час доби спостерігається різна теплова картина місцевості. За результатами експериментальних досліджень визначено, що найкращі теплові зображення об'єктів на місцевості спостерігаються перед сходом Сонця, відповідно можливості знаходження та розрізнення об'єкта на фоні – оптимальні, а найгірші після заходу Сонця.

Прогнозування інтервалів часу доби для використання БПЛА обладнаних ТСС може здійснюватися аналітичним моделюванням або за рахунок проведення експериментальних досліджень з натурних спостережень аналога об'єкта на місцевості за допомогою тепловізійної системи. Проте, у зв'язку з великою кількістю можливих комбінацій об'єктів та фонів, різноманіттям їх теплофізичних і масо-габаритних властивостей та стохастичним характером зміни погодних умов проведення експериментальних досліджень є затратним процесом у часі. Крім того, не завжди є можливість застосування для експериментальних досліджень аналогів об'єктів і фонів.

Аналітичне моделювання інтервалів часу доби є більш гнучким інструментом для вирішення даного завдання. Воно передбачає використання алгоритмів переходу від математичних моделей добових змін температури об'єкту на місцевості і фону до алгоритму з'ясування інтервалів доби. Аналітичне моделювання має враховувати теплофізичнічні, масо-габаритні, географічні, погодні та часові фактори впливу та значення температури об'єкта і фону. Також потребує розроблення методики, що дозволить перейти від оцінювання температурних показників об'єктів і фонів в темний час доби до оцінки якості зображення ТСС. Даний підхід дозволить визначати інтервали часу добу, коли різниця температури об'єкта і фону буде максимально можливою.

Таким чином, використання аналітичного моделювання дозволить прогнозувати інтервали часу доби для проведення тепловізійного спостереження оператором БПЛА. Тепловізійне спостереження в інтервали часу доби, коли ефективність виявлення буде максимально можливою, дозволить збільшить відстань застосування БПЛА для виявляє військової техніки НЗФ. Також, проведення тепловізійного спостереження з БПЛА в інтервали часу доби, коли температурна різниця між об'єктом і фоном максимально можлива дозволить отримувати теплові зображення об'єктів з вищими розпізнавальними властивостями. З іншої сторони, прогнозування інтервалів часу доби дозволить уникати ситуацій, коли виявлення об'єктів на місцевості ускладнене.

Перспективними напрямами досліджень в цій сфері можна назвати такі: розроблення рекомендаційних таблиць щодо вибору часу доби для використання БПЛА обладнаних ТСС; врахування впливу пори року та географічного місця розташування об'єкта на зміну довжини інтервалів часу доби для використання ТСС.

Марфін О.В. (ВІТІ)
Симоненко О.А. (ВІТІ)

АНАЛІЗ ЗАСТОСУВАННЯ ФРЕЙМВОРКІВ ДЛЯ РОЗРОБКИ WEB-ДОДАТКІВ

Актуальність. Кожного разу коли *web*-програміст починає новий проект він стикається з вибором: який *JavaScript* фреймворк вибрати для сайту – *Vue.js*, *React* або *Angular*? Кожен з них підходить для вирішення певних завдань. Тому залишається не вирішене питання ефективності роботи. Непрямий аналіз на сайті *Indeed.com* дає досить цікавий розподіл: *React* 78,1%, *Angular* 21%, *Vue.js* 0,8%.

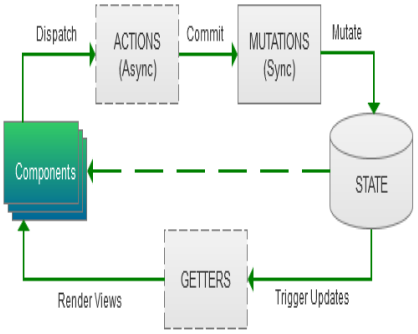


Рис.1. Схема роботи *Angular*

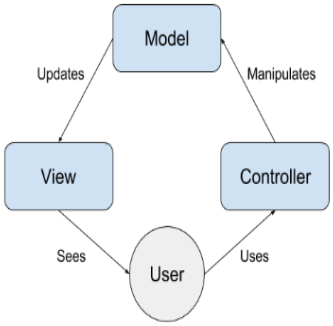


Рис.2. Схема роботи *Vue.js*

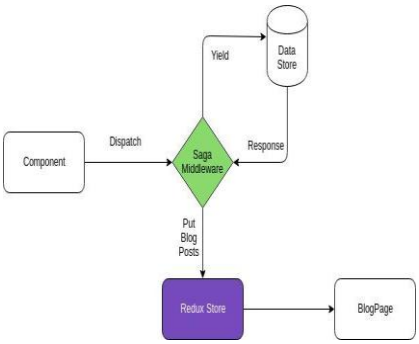


Рис.3. Схема роботи *React*

Мета. Здійснити аналіз *Javascript* фреймворків для використання в різних видах розробки, а також визначити їх сильні сторони.

Виклад основного матеріалу. *Javascript* фреймворки в першу чергу варто порівняти у відображенні сторінки. Сучасна архітектура допускає два види відображення: на стороні клієнта або на стороні сервера. *Vue.js* і *React* створюють копію *DOM*, обробляють її, а потім результат порівнюється з вихідною версією. В кінцевому документі замінюються тільки ті частини сторінки, які відрізняються від результатів обробки. Це значно прискорює завантаження і відображення сторінки. Повністю відрізняється підхід до обробки *DOM* фреймворком *Angular* версії 1.x і вище. Тут відбувається поділ на два потоки, причому за рендеринг *DOM* „відповідає" браузер, а за створення директив, завантаження коду і сервісів – загальний потік. Саме в уніфікації процесів криється популярність повноцінних фреймворків. *React* і *Vue.js* підтримують тільки односторонню передачу даних. При цьому в *React* об'єкти вміщені. Однак *React* підтримує копіювання і передачу стану. Отже, рендеринг буде ідентичним, на екранах обох пристроїв буде одна і та ж „картинка". Фреймворк *Vue.js* працює вже трохи інакше. Є підтримка *JSX*, що спрощує перехід з *React* і схожих бібліотек. Фреймворк *Angular* дещо відрізняється логікою процесу. Так, тут є все, що властиво *Vue.js*, однак опис взаємодії об'єктів відбувається в службах, які є складовими частинами модулів. Модульна архітектура більш зручна при розробці великих додатків. Кінцевий розмір коду стає менше, а швидкість обробки вище. Для розробника додатку важлива можливість відновлення архітектури для підключення нових модулів і бібліотек. ***Angular*** **–** повноцінний фреймворк. Абсолютна залежність від попередніх версій і компонентів. Це призводить до необґрунтованого збільшення обсягу програми. ***React*** **-** бібліотека. Повна сумісність між версіями. Можливе підключення до додатка бібліотек різних версій, оновлення застарілих зі спадкуванням властивостей. ***Vue.js*** **-** прогресивний фреймворк. Модульна система аналогічна *React*, але включає в себе всі атрибути *JS*-фреймворка.

Висновок. Таким чином використання певного фреймворку має свої плюси і мінуси. Якщо потрібно швидко вивчити середу, то варто вибирати між *Vue.js* і *React*. Якщо передбачається розробка великого проекту, то варто розглядати *Angular* в якості основи. Він забезпечує максимальну гнучкість і швидкість рендеринга. Якщо ж потрібно змінювати додаток без руйнування архітектури та обробку і вдосконалення одного проекту декількома спеціалістами, то *Vue.js* стане кращим рішенням.

к.т.н. Масесов М.О. (ВІТІ)

ПЕРСПЕКТИВИ РОЗВИТКУ ВІЙСЬКОВИХ ТРАНСПОРТНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Сучасний розвиток системи військового зв'язку обумовлений безперервним удосконаленням системи управління Збройними силами України. Впровадження сучасних телекомунікаційних послуг (сервісів), систем відеоспостереження, інтеграційних платформ та автоматизованих систем управління висувають зростаючі вимоги щодо якості та пропускної спроможності каналів зв'язку військової телекомунікаційної системи.

Військова транспортна телекомунікаційна мережа, як складова військової телекомунікаційної системи, складається з прямих телекомунікаційних ліній (мереж), військової телекомунікаційної опорної мережі, орендованих каналів передавання і групових трактів. Серед наведених складових доцільно розглянути перспективи розвитку опорної мережі та прямих телекомунікаційних ліній.

Військова телекомунікаційна опорна мережа будується, в основному, з використанням проводових та радіорелейних засобів зв'язку.

В мобільній компоненті в першу чергу використовуються радіорелейні станції для побудови радіорелейних інтервалів та ліній. Новітні цифрові радіорелейні станції, які на теперішній час прийняті на озброєння (постачання) у Збройних Силах України та активно використовуються, представлені такими типами як Р-425, Р-402, Р-450, Р414МУ, RF-7800W.

Перспективним напрямом розвитку радіорелейних станцій на теперішньому етапі розвитку військ зв'язку Збройних Сил України є створення уніфікованих станцій, призначених для роботи у різних ланках управління, що утворюють як високошвидкісні радіорелейні лінії, так і низькошвидкісні лінії прив'язки до телекомунікаційних мереж.

Для забезпечення високої пропускної спроможності у сучасних радіорелейних станціях використовуються перспективні технології, такі як OFDM (Orthogonal Frequency-Division Multiplexing), MIMO 2x2 (Multiple Input Multiple Output – множинний вхід множинний вихід), TDMA (Time Division Multiple Access – множинний доступ з розділення по часу) на базі модифікованих стандартів IEEE 802.11 та 802.16. Використання зазначених технологій у сукупності з сучасною апаратною базою дозволяє передавати будь-які види послуг, як то телефонія, відео у режимі реального часу, відеоконференцзв'язок – що у перспективі дозволяє будувати систему С4ISR відповідно до вимог Стратегічного оборонного бюлетеню.

Крім того, залишається актуальним перехід у верхній діапазон частот (до 80 ГГц), який недоступний для придушення засобами радіоелектронної боротьби противника, а також використання спеціальних синхронних протоколів TDD (Time Division Duplex – дуплексний канал с часовим розділенням).

Розвиток проводових засобів зв'язку спрямовано, в першу чергу, на впровадження волоконно-оптичних систем передавання, особливо у стаціонарній компоненті системи зв'язку Збройних Сил України. Використання волоконної оптики дозволяє не тільки нарощувати пропускну спроможність проводових ліній зв'язку, але й забезпечити надійність та скритність їх використання.

Таким чином, перспективами розвитку військових транспортних телекомунікаціних мереж є використання сучасних радіорелейних засобів та волоконно-оптичних систем передавання, що дозволяє підвищити пропускні спроможності ліній військового зв'язку, забезпечити передавання всіх видів трафіку та послуг, а також створює передумови подальшого розвитку системи військового зв'язку з метою створення перспективної системи управління у відповідності до концепції С4ISR.

к.т.н. Машкін О.О. (ЦНДІ ЗС України)

АЛГОРИТМ СТРУКТУРНОЇ АДАПТАЦІЇ КОМПЛЕКСІВ МАТЕМАТИЧНИХ МОДЕЛЕЙ ОПЕРАЦІЙ (БОЙОВИХ ДІЙ) В УМОВАХ ЧАСОВИХ ОБМЕЖЕНЬ НА ОТРИМАННЯ РЕЗУЛЬТАТІВ РОЗРАХУНКІВ

Актуальність теми. Комплекс математичних моделей бойових дій та операцій угруповань військ (КММ операцій) є дієвим та потужним інструментом підтримки та обґрунтування рішень, що приймаються у органах військового управління та оперативних штабах. Практикою багаторазового застосування дослідного зразка КММ операцій на заходах оперативної підготовки встановлено, що загалом на таких заходах може проводитись близько 100 різноманітних розрахунків, з яких біля 20 можна віднести до основних. Іншою особливістю експлуатації КММ операцій на таких заходах слід вважати достатньо жорсткі обмеження, що накладаються на час отримання потрібних результатів. Як правило, комплекси подібного призначення будуються з урахуванням вимог можливості їх розгортання на різнотипних обчислювальних засобах та мережах. Так, згаданий КММ операцій може бути встановлений як на локальну ПЕОМ, так і розгортатися на різнорангових локальних мережах. Є зрозумілим, що швидкість отримання результатів моделювання залежатиме від багатьох факторів, серед яких можна виділити: обсяг даних, що підлягатимуть обробці; особливості програмної реалізації моделей комплексу; характеристики продуктивності ПЕОМ та фізичну топологію мережі у разі її розгортання. Тобто, комплекс моделей можна розглядати як складну багатоструктурну технічну систему, відповідно, постановкою завдання дослідження слід вважати обґрунтований вибір такої конфігурації (насамперед – модельно-алгоритмічної структури) КММ операцій, яка забезпечить проведення необхідного обсягу розрахунків за встановлений час. В такому випадку метою досліджень є побудова алгоритму структурної адаптації комплексу моделей до поточних умов та завдань на проведення оперативних розрахунків.

Комплекси моделей, призначених для відображення можливого ходу та результатів такого складного процесу як операція, зазвичай включають до свого складу різнотипні моделі (розрахункові задачі), що описують один процес. Найбільш типовим прикладом можна вважати наявність у комплексі аналітичних та імітаційних моделей, спрощену альтернативу вибору яких можна представити у вигляді: швидкість отримання усереднених результатів, або достовірність та наочність отриманих результатів. Алгоритм вибору конкретної моделі зі складу комплексу повинен ураховувати прогнозний час, що буде витрачений на проведення моделювання з урахуванням перелічених вище ключових факторів та обмежень за часом. Встановлення залежності, яка пов’язує час моделювання з характеристиками технічної структури КММ (наявні ПЕОМ та їх продуктивність), характеристиками технологічної структури (перепускна спроможність мережі), особливостями модельно-алгоритмічною структури, доцільне шляхом використання арсеналу методів аналізу даних, зокрема – нелінійного регресійного аналізу. Вихідними даними для побудови регресійної моделі слугуватиме оброблена статистика результатів функціонування моделей для найбільш типових конфігурацій технічної та технологічної структур комплексу при застосуванні КММ в межах наступних основних цілей: проведення оперативних розрахунків; детальне імітаційне моделювання; навчання особового складу органів військового управління. Отримана регресійна модель є ключовим елементом в роботі алгоритму структурної адаптації комплексу моделей, при цьому алгоритмом повинна бути урахована можливість організації паралельних або розподілених обчислень (при відповідній конфігурації технічної та технологічної структур комплексу). В якості **висновку** можна зазначити, що програмна реалізація у модулі управління КММ операцій розробленого алгоритму дозволить у автоматизованому режимі адаптувати модельно-алгоритмічну структуру комплексу до поточних умов та завдань його застосування.

к.військ.н. Микусь С.А. (НУОУ)
к.військ.н. Войтко О.В., (НУОУ)
к.т.н. Мазулевський О.Є. (ВІТІ)

ОСНОВНІ НАПРЯМИ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ У КІБЕРПРОСТОРІ (ЧЕРЕЗ КІБЕРПРОСТІР) МІНІСТЕРСТВОМ ОБОРОНИ ТА ЗБРОЙНИМИ СИЛАМИ З УРАХУВАННЯМ СТАНДАРТІВ НАТО

Стрімкий розвиток інформаційних технологій трансформує світ. Крім корисних функцій розвиток дістається і негативних – поширюються випадки незаконного збирання, зберігання, використання, знищення, поширення, персональних даних, незаконних фінансових операцій, крадіжок та шахрайства у мережі Інтернет. Кіберзлочинність стає транснаціональною та здатна завдати значної шкоди інтересам особи, суспільства і держави.

Кіберпростір поступово перетворюється на окрему, поряд із традиційними „Земля", „Повітря", „Море" та „Космос", сферу ведення бойових дій, у якій все більш активно діють відповідні підрозділи збройних сил провідних держав світу. Наприклад Пентагон США у 2015 році розробив „Стратегію дій міністерства оборони США в кіберпросторі", яка визначила основні напрямки розвитку кіберпотенціалу збройних сил та вимоги до нього.

Основною потенційною загрозою в кіберпросторі є те, що окремі держави і недержавні структури здійснюють протиправну діяльність, проникаючи в інформаційні мережі та системи інших держав з різними цілями: отримання таємної та конфіденційної інформації, крадіжка інтелектуальної власності, перешкоджання веденню бізнесу комерційним організаціям, проведення руйнівних кібератак тощо.

На думку світових експертів одними із країн, які ведуть активні дії в кіберпосторі названі Росія, Китай, Північна Корея і Іран, Ізраіль, США. Крім того, загрозу національним інтересам країн представляють недержавні структури, такі як наприклад терористична організація „Ісламська держава Іраку і Лівану" (ІДІЛ), які використовують можливості киберсистем для вербування послідовників, бойовиків та пропаганди своїх ідей і цінностей. Кіберресурси також широко застосовують кримінальні угруповання, завдаючи шкоди насамперед фінансовому сектору.

Тому основними пріоритетними (стратегічними) цілями в кіберпросторі є:

– нарощування та підтримання можливостей сил та для проведення операцій в кіберпросторі;

– захист інформаційних мереж та баз даних МО та ЗС України, а також зниження ризиків для виконання задач МО та ЗС України;

– бути в готовності до захисту національних і життєво важливих інтересів держави від руйнівних або деструктивних кібератак із значними наслідками.

– планування застосування кіберсил для забезпечення контролю конфліктів і формування вигідної обстановки на всіх етапах їх розвитку.

– створення та підтримання міцних міжнародних альянсів і організацій для стримування загроз та збільшення міжнародної безпеки та стабільності.

В цих умовах постала нагальна потреба створення та розвитку власної дієвої системи забезпечення кібербезпеки.

5 жовтня 2017 року був прийнятий Закон України „Про основні засади забезпечення кібербезпеки України", який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Відповідно основними завданнями Міністерства оборони та Збройних сил України в національній системі кібербезпеки є:

– здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони);

– здійснення військової співпраці з НАТО, пов'язаної з безпекою кіберпростору та сумісним захистом від кіберзагроз;

– забезпечення, у взаємодії з Державною службою спеціального зв'язку та захисту інформації України та Службою безпеки України, кіберзахисту власної інформаційної інфраструктури.

Для виконання зазначених завдань на Міністерство оборони та Збройні сили України необхідно покласти виконання ряду основних заходів дій у кіберпросторі (через кіберпростір):

1. Невійськові дії:

– кіберрозвідка (CYBERINTOPS);

– забезпечення бізнес-процесів (повсякденної діяльності) Міністерства оборони України та Збройних Сил України в кіберпросторі (BUSINESSOPS).

2. Військові дії (операції) з кібероборони (CYBER DEFENCE):

– кіберзахист (технічний захист інформації) систем електронної комунікації (поєднання дій (операцій) в кіберпросторі інформаційної безпеки (INFOSEC „INFORMATION SECURITY"), безпеки операцій (OPSEC „OPERATIONAL SECURITY"): виявлення впливу кібератак на безпеку систем електронної комунікації; попередня ідентифікація кібератак; розробка способів боротьби з кібератаками (кібервпливами); кіберзахист в системах супутникової навігації та топогеодезичного забезпечення, які використовують космічні інформаційні технології та інш.;

– активні дії в кіберпросторі (поєднання дій (операцій) психологічних операцій в кіберпросторі (PSYOPS, „PSYCHOLOGIC OPERATIONS"), введення в оману (MILDEC, „MILITARY DECEPTION"), радіоелектронної боротьби (CEW, „CYBER ELECTROMAGNETIC WARFARE"): моніторинг соціальних мереж щодо виявлення негативного інформаційно-психологічного впливу на особовий склад; моніторинг інших сегментів кіберпростору та виявлення негативного інформаційно-психологічного впливу через кіберпростір; проведення спеціальних дій в кіберпросторі; порушення функціонування об'єктів інформаційної інфраструктури противника; впровадження спеціальних програмних засобів в інформаційно-телекомунікаційні системи противника; проведення дій (операцій) в кіберпросторі з введення противника в оману; блокування в кіберпросторі джерел деструктивного програмно-математичного впливу на інформаційну інфраструктуру Міністерств оборони України та інформаційно-телекомунікаційні системи Збройних сил України та інш.);

– забезпечення функціонування ІТ-систем (електронних комунікацій), а саме: забезпечення кібербезпеки особового складу та кіберзахисту електронних комунікацій у Збройних Силах України; здійснення в особливий період контролю підготовки систем електронних комунікацій до кібероборони та використання кіберпростору; побудови та забезпечення функціонування системи захисту інформації в інформаційно-телекомунікаційних системах; основні положення щодо реагування на інциденти кібербезпеки в інформаційно-телекомунікаційних системах та їх запобігання; реагування на кібератаки у режимі реального часу; усунення наслідків впливу кібератак (після їх ідентифікації); розміщення антивірусних оновлень на виділених ресурсах автоматизованих систем класу „3"; забезпечення функціонування серверів антивірусного захисту; оновлення сигнатур кібератак в засобах кібербезпеки; фізичний захист критичних елементів інформаційно-телекомунікаційних систем та інш.

Виконання зазначених заходів дій дозволить побудувати ефективну систему забезпечення кібербезпеки Міністерства оборони та Збройних сил України, як складової національної системи кібербезпеки, що в свою чергу дасть можливість своєчасно реагувати на гібридні кіберзагрози.

Мирончук О.Ю. (РТФ НТУУ „КПІ”)
к.т.н. Шпилька О.О. (РТФ НТУУ „КПІ”)

МОДЕЛЮВАННЯ КАНАЛІВ ЗВ’ЯЗКУ ІЗ ЗАДАНИМИ КОРЕЛЯЦІЙНИМИ ВЛАСТИВОСТЯМИ

Вступ. При проектуванні систем зв’язку важливим етапом являється вибір моделі каналу зв’язку. Математична модель дозволяє відобразити найбільш важливі характеристики фізичного середовища, через яке проходить сигнал. На основі моделі виконується дослідження впливу каналу на сигнал, що є необхідним при виборі методу модуляції і способу кодування. Технічні характеристики сучасних ЕОМ дозволяють повністю змоделювати роботу системи зв’язку, що дає можливість протестувати нові ідеї та підходи ще на етапі проектування.

Основні положення. Під час поширення через безпровідний канал зв’язку сигнал зазнає впливу явища багатопроменевого поширення радіохвиль. Це явище виникає внаслідок їх відбиття, дифракції та розсіювання від перешкод на шляху поширення. В залежності від значень часових затримок поширення в точці прийому сигнали, що проходять різними шляхами, можуть складатися як у фазі, так і протифазі. В свою чергу, це приводить до утворення завмирань на певних значеннях частоти. В якості моделі каналів з багатопроменевим поширенням широко використовується гаусівський випадковий процес - випадковий процес з нормальним законом розподілу ймовірностей [1].

Одним із методів формування гаусівського випадкового процесу з заданими кореляційними властивостями являється використання формуючого фільтра [2]. Цей метод базується на двох положеннях теорії випадкових процесів:

1. Результатом лінійного перетворення гаусівського випадкового процесу являється також гаусівський випадковий процес.
2. Спектральні густини потужності випадкових процесів на вході і виході лінійного фільтра з частотною характеристикою $H(j\omega)$ зв’язані співвідношенням:

$$S_{вих}(\omega)=|H(j\omega)|^2 S_{вх}(\omega). \quad (1)$$

Якщо на вхід фільтра поступає випадковий процес у вигляді білого шуму, то спектральна густина потужності процесу на виході буде рівна

$$S_{вих}(\omega)=S_0|H(j\omega)|^2, \quad (2)$$

де S_0 - спектральна густина потужності білого шуму.

Таким чином, для формування гаусівського випадкового процесу з заданою спектральною густиною потужності необхідно мати фільтр, модуль частотної характеристики якого визначається як

$$|H(j\omega)|=\sqrt{\frac{S_{вих}(\omega)}{S_0}}. \quad (3)$$

Вираз (3) дає можливість розрахувати амплітудно-частотну характеристику (АЧХ) фільтра і не визначає його фазо-частотну характеристику (ФЧХ).

Теорема Вінера-Хінчіна стверджує, що спектральна густина потужності стаціонарного випадкового процесу являється перетворенням Фур’є від автокореляційної функції цього процесу [3]

$$S(\omega)=\int_{-\infty}^{\infty} R(\tau)e^{-j\omega\tau}d\tau. \quad (4)$$

Виходячи з цього, алгоритм формування гаусівського випадкового процесу з заданими кореляційними властивостями наступний:

1. Формування випадкового процесу у вигляді білого шуму зі спектральною густиною потужності S_0.

2. Формування необхідної автокореляційної функції випадкового процесу на виході фільтра $R(\tau)$.

3. Розрахунок спектральної густини потужності випадкового процесу, який має бути на виході формуючого фільтра.

4. Розрахунок передаточної функції формуючого фільтра $H(j\omega)$.

5. Виконання фільтрації та перехід від спектральної густини потужності до часових відліків вихідного процесу.

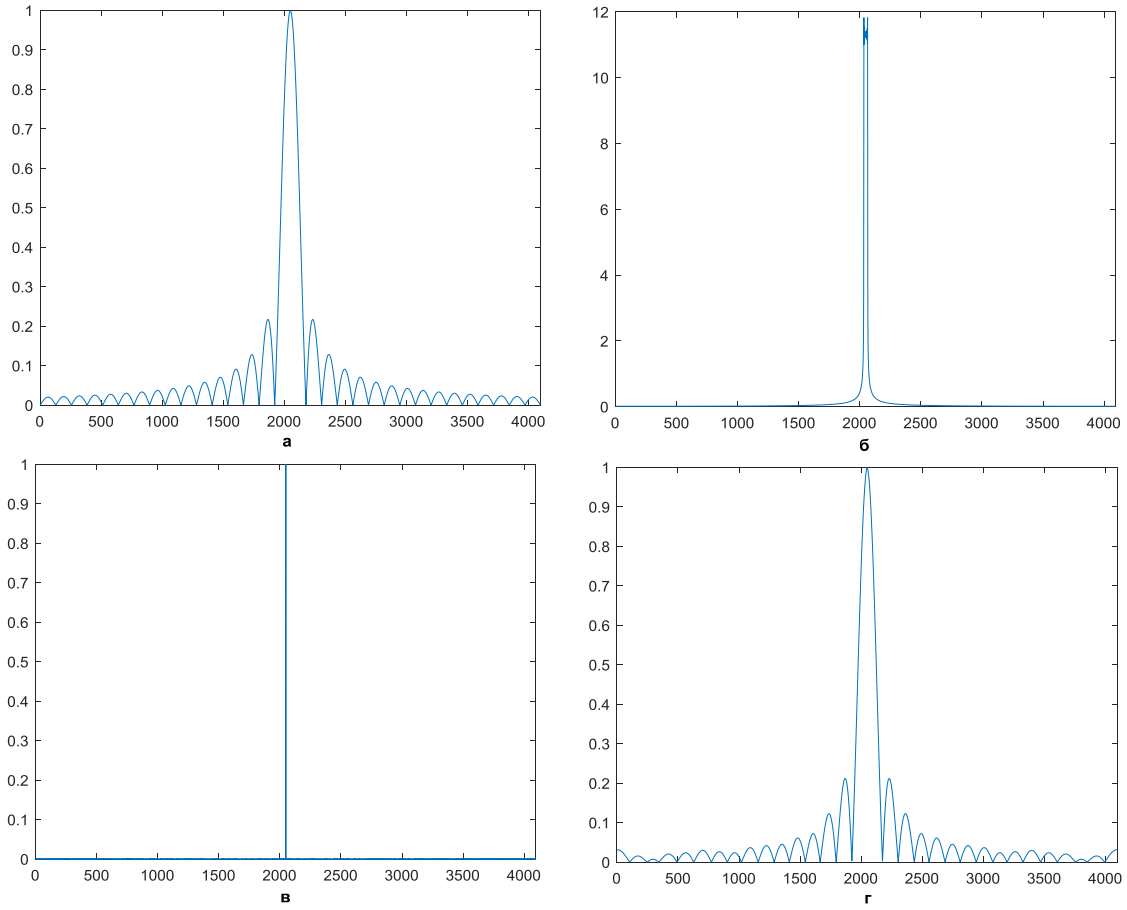


Рис.1 Результати моделювання

На Рис. 1 відображено результати моделювання описаним вище алгоритмом. Необхідна автокореляційна функція випадкового процесу на виході формуючого фільтра представлена на Рис. 1а. Модуль передаточної функції формуючого фільтра представлений на Рис. 1б. Автокореляційна функція білого шуму на вході формуючого фільтра представлена на Рис. 1в. Автокореляційна функція випадкового процесу на виході формуючого фільтра представлена на Рис. 1г.

Висновки. Розглянутий метод формування випадкового процесу з заданими кореляційними властивостями, в основі якого лежить використання формуючого фільтра, являється простим і ефективним для моделювання каналів зв'язку.

ЛІТЕРАТУРА

1. Левин Б. Р. Теоретические основы статистической радиотехники. – 3-е над.., перераб. и доп. – М.: Радио и связь, 1989. – 656 с.

2. Быков В. В. Цифровое моделирование в статистической радиотехнике. Изд-во „Советское радио", 1971, 328 стр.

3. Гоноровский И. С. Радиотехнические цепи и сигналы: Учебник для вузов.– 4-е изд., перераб. и доп. – М.: Радио и связь, 1986. – 512 с.

Михалевич В.Е. (ЦНДІ ЗС України)

ПІДХІД ДО МОДЕЛЮВАННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ АСУ В ОПЕРАЦІЇ ОПЕРАТИВНОГО УГРУПОВАННЯ ВІЙСЬК

Останнім часом у Збройних силах України значна увага приділяється процесам інформатизації та впровадження автоматизованих систем управління (АСУ) різного рівня та призначення. Такий акцент, в першу чергу, спрямовано на підвищення ефективності управління за рахунок підвищення оперативності отримання даних, їх повноти та зменшення впливу людського фактору. Але, разом з цим, з'являються додаткові особливості, пов'язанні із зростанням складності програмно-апаратного та алгоритмічного забезпечення АСУ. Під час підготовки до проведення та безпосереднього ведення операцій (бойових дій) для АСУ військового притаманні певні особливості функціонування. Насамперед, противник намагається вплинути на інформаційно-телекомунікаційне забезпечення, основну складову системи управління. Крім того, існує стійка тенденція збільшення обсягів інформації, що передається. Враховуючи зазначені особливості функціонування АСУ військового призначення, виникає необхідність дослідження функціонування ІТЗ АСУ в умовах проведення операцій (бойових дій).

Таким чином, можна вважати, що ІТЗ АСУ належить до класу складних ієрархічних динамічних просторово-розподілених систем (ПРС). Одним з доступних методів для дослідження таких систем є математичне моделювання. У сучасній літературі, як правило, розглядається коефіцієнтний підхід урахування ІТЗ, який є дуже наближеним. Тому, розгляд підходу до моделювання інформаційно-телекомунікаційного забезпечення АСУ операції оперативного угруповання військ є актуальним.

Аналіз існуючих математичних моделей (методик) свідчить, що моделювання ІТЗ, зазвичай, представляється у матричному вигляді (матриці: зв'язності, досяжності, контрдосяжності, вагів тощо) або системи масового обслуговування. При цьому вирішується набір оптимізаційних задач. Як правило, обираються часткові показники ефективності, які дають відповідь щодо відповідності меті функціонування системи, що є достатнім. Однак, якщо застосувати системний підхід і розглядати ІТЗ, як елемент системи вищого рівня, то оцінити вплив показників ефективності функціонування ІТЗ (швидкості передачі повідомлень, імовірності передачі повідомлення, часу затримки повідомлення, повноти та адекватності інформації, зв'язності, стійкості тощо) на хід та результати операції (бойових дій) в цілому достатньо складно.

У підході, який розглядається, пропонується аналітична стохастична математична модель ІТЗ, що інкапсулює в собі низку математичних моделей, зокрема:

– статичні оптимізаційні моделі ПРС (знищення елементів ІТЗ ракетними військами і артилерією, механізованими (танковими) військами, авіацією; подавлення радіоелементів телекомунікаційної мережі силами та засобами РЕБ);

– динамічні оптимізаційні моделі ПРС (маршрутизації пакетів; розподілу мережевого ресурсу відповідно до категорії важливості повідомлень; визначення адекватності інформації умовам обстановки; зміни топології мережі).

Зважаючи на складність формалізації процесів управління військами, під час проведення досліджень прийняті такі вихідні дані: розглядається область управління вогнем для змішаних угруповань; інформація – сукупність структурованих даних для автоматизованого формування вектору засобів ураження та вектору цілей; розглядається лише маршрутизація пакетів; потік надходження пакетів – за законом розподілу Пуассона.

Таким чином, запропонований підхід до моделювання інформаційно-телекомунікаційного забезпечення АСУ в операції оперативного угруповання військ деталізує результати моделювання операцій військ за показниками ефективності ОУВ, що значно підвищує їх точність та достовірність.

Михальчук І.І.(ВІТІ)
Стаценко В.І.(ВІТІ)

АДАПТИВНА СИСТЕМА АВТОМАТИЗОВАНОЇ ПЕРЕВІРКИ (ТЕСТУВАННЯ) ЗНАНЬ КУРСАНТІВ

АСКЗ – передбачає програмно-апаратний комплекс, призначений для проведення викладачем(офіцером) оцінки успішності курсантів(солдатів) шляхом проведення тестового опитування засобами ЕОМ, для об'єктивної оцінки рівня їх знань в певній предметній області з автоматизованим процесом оцінювання.

Система створена для оптимізації та автоматизації навчального процесу у вищих військових закладах та у військах. АСКЗ набуває все більшого поширення в навчальному процесі та під час відпрацювання теоретичних навичок, завдяки автоматизації отримання результатів та певним додатковим умовам проведення тестового контролю його застосування оптимізує можливість об’єктивної оцінки рівня фахової підготовки курсанта.

Представлено порівняльні характеристики та аналіз вже існуючих технологій автоматизованої перевірки знань та можливість розробки та використання системи автоматизованої перевірки (тестування).

З активним впровадженням досягнень інформаційних технологій в навчальний процес з’явилася можливість використовувати комп’ютерне тестування не лише при поточному чи проміжному контролі, а і при рубіжному та підсумковому контролі якості засвоєння навчального матеріалу курсантами.

Тому постає актуальна наукова задача щодо розробки системи автоматизованої перевірки (тестування) знань курсантів, що в свою чергу приведе до збільшення ефективності навчального процесу курсантів.

Система несе в собі широкий спектр дидактичних функцій, а також виконує всі функції засобів навчання: компенсаторну функцію, адаптивну функцію, організацію демонстрацій, самостійних робіт, адекватність змісту поняття віковим можливостям курсантів, функцію інформативності, інтегративну функцію, інструментальну функцію.

Проектування системи з міркувань зручності і універсальності підходу було реалізовано на основі *WEB*-інтерфейсу, з використанням локального *WEB* - сервера *XAMPP*.

Тестування показало, що відповідне ПЗ забезпечує надійну взаємодію та при цьому не потребує значних затрат обчислювального ресурсу, що позитивним чином впливає на швидкодію інформаційної системи вцілому.

Основними вимогами до АСКЗ можна визначити:

- Можливість працювати з будь-якими типами тестових завдань
- Можливість АСКЗ працювати в різних режимах роботи (тренінг, самоконтроль, контроль)
- АСКЗ повинно забезпечувати формування банку тестових завдань
- АСКЗ повинна дозволяти створювати тест, що складається з тестових завдань, взятих із різних наборів
- В АСКЗ повинна передбачатись можливість зміни параметрів автоматичного формування тесту з набору тестових завдань
- Викладач повинен мати можливість в процесі контролю за допомогою АСКЗ адаптувати складність тестових завдань
- АСКЗ повинна дозволяти формувати алгоритм обчислення результуючого балу з використанням певної шкали

Таким чином дана адаптивна система автоматизованої перевірки (тестування) знань курсантів допоможе об'єктивно оцінити рівень знань курсантів (солдатів) в певній предметній області з автоматизованим процесом оцінювання.

д.т.н. Могилевич Д.І. (ВІТІ)
к.т.н. Кононова І.В. (НТУУ „КПІ ”)

АНАЛІЗ МЕТОДІВ ПІДВИЩЕННЯ НАДІЙНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМ УПРАВЛІННЯ ВІЙСЬКАМИ ТА ОЗБРОЄННЯМ

Революційні процеси комп’ютеризації та інтелектуалізації систем управління військами (силами) та озброєнням призвело до різкого збільшення об’ємів та складності програмного забезпечення (ПЗ). Як наслідок, до теперішнього часу склалася ситуація, коли бойові можливості і стійкість систем управління військамі та сучасної зброї визначаються показниками якості та надійності не тільки апаратних засобів, але й ПЗ. Програмне забезпечення стає джерелом уразливості сучасних військових систем, а використання програмних засобів у складі систем зброї, бойового управління та зв’язку породжує нову задачу – забезпечення технологічної безпеки програмних засобів військового призначення.

Ускладнення програмного забезпечення стає причиною появи в ньому значної кількості програмних помилок, наявність яких призводить до зниження рівня надійності програмного забезпечення і ефективності бойового застосування складних військово-технічних систем.

У міжнародному стандарті *ISO* 9126:1991 надійність виділена як одна з шести основних характеристик якості ПЗ разом з функціональною придатністю, застосовуваністю, ефективністю, сопроводжуваністю та переносимістю. Відповідно до стандартного словника термінів програмного інжинірингу надійність програмного забезпечення це здатність системи або компонента виконувати необхідні функції в заданих умовах протягом зазначеного періоду часу.

Для забезпечення надійності ПЗ запропоновано безліч підходів, але відсутність загальновизнаних критеріїв надійності не дозволяє відповісти на питання, наскільки надійніше стає програмне забезпечення при дотриманні процедур та технологій, що пропонуються та в якій мірі виправдані витрати. Таким чином, пріоритет задачі оцінки надійності повинен бути вище пріоритету завдання її забезпечення, проте на практиці це відбувається.

Аналіз існуючих моделей надійності програмного забезпечення (моделі Шумана, Ла Падула, Джелінського-Моранді, Шика-Волвертона, Муса, Мілса, Ліпова, Коркорена, Нельсона, модель прехідних ймовірностей, проста інтуїтивна модель і ін.) показує, що вони є неадекватними в реальному процесі функціонування програмного забезпечення складних військово-технічних систем. Перш за все, це пов’язано з тим, що наявні моделі надійності ПЗ мають надмірну кількістю обмежень та допущень. Крім того, в кожній з моделей, час безвідмовної роботи програмного забезпечення підпорядковується якомусь конкретному закону розподілу, який практично неможливо підтвердити у разі неповної статистичної інформації щодо програмних помилок. Тому жодна із запропонованих моделей не використовується на практиці, так як їх застосування незручне або недоцільне.

Між програмними помилками, відмовами та надійністю ПЗ можна виділити деякі закономірності і фактори, які впливають на надійність ПЗ: набір вхідних даних і тривалість випробувань ПЗ впливають на показники надійності ПЗ; програмні помилки виявляються з різною частотою, а також кілька програмних помилок можуть проявлятися одночасно; не кожна програмна помилка може бути виявлена та виправлена, оскільки проявляються не самі програмні помилки, а їх результат – відмова; програмні помилки можуть впливати одина на одну, тому після виправлення однієї програмної помилки можуть бути внесені інші. І як результат надійність програмного забезпечення може стати нижче, ніж до виправлення цієї програмної помилки; відмова програмного забезпечення може бути наслідком не однієї, а відразу декількох програмних помилок, проте не кожна програмна помилка може призвести до відмови програмного забезпечення.

Проведене дослідження показало, що першопричиною порушення працездатності програм при безвідмовності апаратури завжди є конфлікт між реальними вихідними даними, що підлягають обробці, і програмою, яка здійснює цю обробку. Працездатність ПЗ можна гарантувати при конкретних вихідних даних, які використовувалися при налагодженні та випробуваннях. Реальні вихідні дані можуть мати значення, що відрізняються від заданих технічним завданням і від використаних при застосуванні програм. При таких вихідних даних функціонування ПЗ важко передбачити заздалегідь, і дуже ймовірні різні аномалії, що завершуються збоями (відмовами).

Непередбачуваність виду, місця і часу прояви відмов (збоїв) в процесі експлуатації ПЗ призводить до необхідності розробки та застосування спеціальних, додаткових методів оперативного підвищення надійності ПЗ (оперативного захисту від ненавмисних, випадкових спотворень обчислювального процесу, програм і даних), які призначені для виявлення та блокування поширення негативних наслідків прояву відмов (збоїв) і зменшення їх впливу на надійність функціонування апаратних засобів до усунення їх первинних джерел. Для цього в ПЗ доцільно вводити часову, інформаційну та програмну надлишковість, що дозволяє здійснювати оперативне виявлення дефектів (відмов, збоїв) функціонування, їх ідентифікацію та автоматичне відновлення (рестарт) нормального функціонування ПЗ.

Під часової надлишковістю розуміють використання деякої частини продуктивності комп'ютера для контролю виконання програм, виявлення спотворень, їх діагностику і рішень щодо відновленню обчислювального процесу або інформації. Для цього при проектуванні інформаційної системи повинен передбачатися запас продуктивності, який буде потім використовуватися на контроль і оперативне підвищення надійності функціонування. Величина часової надлишковості залежить від вимог щодо надійності і знаходиться в межах від 5 – 10 % продуктивності комп'ютера до 3 – 4-кратного резервування продуктивності окремої машини в багатопроцесорних обчислювальних системах.

Інформаційна надлишковість полягає у резервуванні накопичених вихідних та проміжних даних, що обробляються програмами. Надлишковість використовується для забезпечення достовірності даних, які найбільшою мірою впливають на нормальне функціонування ПЗ та вимагають значного часу для відновлення. Їх захищають 2–3-х кратним резервуванням з періодичним оновленням.

Програмна надлишковість використовується для контролю і забезпечення достовірності найбільш важливих рішень щодо обробки інформації. Вона полягає у зіставленні результатів обробки однакових вихідних даних програмами, які відрізняються алгоритмами, що використовуються і у виключенні спотворень при розбіжності результатів.

Програмна надлишковість необхідна також для реалізації програм автоматичного контролю і відновлення даних з використанням інформаційної надлишковості та для функціонування всіх засобів забезпечення надійності, що використовують часову надлишковість. Засоби оперативного програмного контролю включаються після використання прикладних і сервісних програм, тому засоби програмного контролю зазвичай не можуть безпосередньо виявити причину виникнення спотворення обчислювального процесу або даних та фіксує тільки наслідки первинного спотворення, тобто вторинну помилку. Результати первинного спотворення можуть набути катастрофічний характер при запізненні їх виявлення та локалізації.

Таким чином, для забезпечення надійності ПЗ, збої потрібно виявляти з мінімальним запізненням, при цьому бажані мінімальні витрати апаратних ресурсів, тому доцільно використати ієрархічні схеми контролю, при яких послідовно використовується кілька методів в порядку поглиблення контролю і збільшення витрат до виявлення джерела спотворення, а також акцентувати ресурси на виявлення потенційно небезпечних збоїв та досить частих режимів відновлення: при спотвореннях програм і даних, при перевантаженні за продуктивністю і при паралельному використанні програм.

Ефективність застосування методів оперативного підвищення надійності ПЗ істотно залежить від виділених обчислювальних ресурсів на їх реалізацію.

д.т.н. Могилевич Д.І. (ВІТІ)
к.т.н. Кононова І.В. (НТУУ „КПІ ”)

МЕТОДИКА ОРГАНІЗАЦІЇ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ СКЛАДНОЇ ТЕХНІЧНОЇ СИСТЕМИ

Необхідність проведення технічного обслуговування (ТО) виникає на етапі експлуатації будь-якої технічної системи. Головна мета обслуговування полягає в забезпеченні максимальної ефективності від використання системи в процесі експлуатації. Ця мета може бути досягнута цілеспрямованим втручанням у функціонування системи шляхом раціонального вибору виду ТО, обгрунтування оптимальних термінів проведення та змісту обслуговування (комплексу попереджувально-відновлювальних робіт).

Отже, завдання оптимального виду ТО полягає у виборі такої стратегії організації обслуговування, при якій забезпечуються екстремальні значення обраного показника (показників) якості функціонування системи. В якості такого показника зазвичай приймається функціонал, визначений на множині можливих траєкторій випадкового процесу $x(t)$, що описує функціонування системи, і отже, залежить від функцій розподілу напрацювання до відмови об'єкта або окремих його частин (підсистем), часу відновлення і інших характеристик, що визначають стратегію ТО. У завданнях ТО розглядається кілька показників якості, основними з яких є коефіцієнт технічного використання $K_{\text{тв}}$ (комплексний показник надійності) та середні питомі витрати C, тобто витрати, що припадають на одиницю часу перебування системи в підмножині працездатних станів (вартісний показник).

Серед безлічі питань, які впливають на вибір стратегії організації раціонального ТО складної технічної системи, необхідно виділити питання обгрунтування раціональних значень параметрів, що характеризують часові режими обслуговування (періодичність проведення і тривалість виконання), а також технології виконання (перелік робіт з обслуговування, черговість їх виконання, залучені сили та засоби і т.п.). Для вирішення цих питань пропонується наступна методика:

1. Проведення аналізу структури системи та її декомпозиція на окремі функціонально завершені підсистеми, кожна з яких вирішує локальну задачу, спрямовану на досягнення поставленої мети системою в цілому.
2. Складання структурної схеми надійності системи.
3. Визначення (за даними випробувань і (або) дослідної експлуатації) законів розподілу вихідних випадкових величин, а також параметрів цих законів.
4. Вибір найбільш доцільного виду ТО (періодичного або за технічним станом) і моделі обслуговування для кожної підсистеми, виходячи з її призначення, характеру вирішуваних завдань, режиму роботи, характеристик контролю та індикації відмов.
5. Визначення оптимальних значень періодичності та відповідних їм оптимальних значень обраних показників якості обслуговування для кожної підсистеми.
6. Поєднання за часом окремих операцій ТО кожної підсистеми в загальний комплекс заходів обслуговування системи в цілому.
7. Оцінка впливу відхилення від оптимальних значень періодичності обслуговування на вибрані показники якості. Визначення раціональних способів організації та режимів обслуговування кожної підсистеми.
8. Розрахунок показників якості ТО системи за обчисленими значеннями показників для кожної підсистеми.
9. Визначення оптимального методу організації і режиму ТО системи в цілому. Розрахунок загальної тривалості робіт, пов’язаних з обслуговуванням системи. Визначення максимально допустимого часу переведення системи з режиму ТО в основний (робочий) режими.

Таким чином, запропонована методика дозволяє забезпечити основну мету ТО – підтримку необхідного рівня безвідмовності складних технічних систем в реальних умовах експлуатації на основі прогнозування і запобігання деякої частини потенційних відмов.

к.т.н. Молдован В.Д. (ВДА)
Кінах М.О. (ВДА)

ЗАХИСТ ІНФОРМАЦІЇ В СУЧАСНИХ СМАРТФОНАХ З ОПЕРАЦІЙНОЮ СИСТЕМОЮ ANDROID

Актуальність. На сьогодні смартфони стали невід'ємною складовою життя людини. Станом на 2018 рік 45 % відсотків українців є постійними користувачами смартфоніві має місце чітка тенденція щодо їх зростання. Сматрфони мають такі переваги, як широкий спектр послуг комунікації (голосова телефонія, обмін СМС та ММС повідомленнями, користування програмами-месенджерами тощо), мобільність та зручність користування, висока функціональність (на рівніперсональних комп'ютерів), доступ до мережі Інтернет, висока швидкість прийому/передачі даних в мережах стільникового зв'язку(наприклад, у мережах 4G до 1 Гбіт/с). Проте, окрім зручності та багатьох технічних можливостей, вони несуть за собою все більшу загрозу для інформації, що зберігається та передається.

Постановка задачі. На сьогодні проблема захисту інформації у смартфонах стає дедалі актуальнішою. При цьому, для ефективного захисту конфіденційної інформації, необхідно розуміти види та сутність самих загроз для інформації.

Мета. Метою доповіді є визначення та аналіз існуючих загроз безпеці інформації для сучасних смартфонів та на його основі визначення можливих методів захисту та протидії цим загрозам.

Основні положення. На сьогодні найпоширенішою операційною системою (ОС) для смартфонів є Android. Ця платформа є відкритою і швидко розповсюджується через зручний інтерфейс, багатофункціональність, можливість налаштування системи. До головних загроз для смартфонів з ОС Android можна віднести наступні:

шкідливе ПЗ – мобільні аналоги комп'ютерних вірусів, троянських програм тощо;

атаки через додатки і мережі, які, як правило, використовують вразливості браузерів смартфонів та намагаються встановити шкідливе програмне забезпечення (ПЗ) або викрасти конфіденційні дані, що містяться в браузері;

атаки з використанням соціальної інженерії з метою отримання конфіденційної інформації від користувачів або встановлення шкідливого ПЗ;

витік даних (дані про облікові записи користувача, історія смс-листування, контакти, дані, що містяться на карті пам'яті, дані платіжних карток тощо). Крім того, смартфони часто використовуються і для збереження та передачі службової інформації, витік якої може завдати шкоди не тільки власнику смартфона, а й установі, де він працює;

Також слід пам'ятати і про відкритість самого бездротового середовища. Оскільки дані передаються в радіоефірі, то немає ніякого фізичного бар'єра, який би перешкодив зловмиснику отримати до них доступ за умови виконання геометричної, енергетичної, структурної доступностей до радіосигналів, що випромінює смартфон.

Окреслимо ряд практичних рекомендацій щодо захисту від загроз інформаційній безпеці смартфонів, а саме:

не зберігати важливу (конфіденційну) інформацію в смартфоні та на карті пам'яті;

встановлювати додатки тільки з GooglePlay-маркету та регулярно їх оновлювати;

встановити надійне антивірусне програмне забезпечення;

уникати підключення до відкритих і ненадійних мереж Wi-Fi

не залишати смартфон без нагляду та встановити блокування екрану;

у разі виникнення підозри щодо витоку інформації через смартфон, повернути його до заводських установок.

Висновок. Таким чином, в доповіді визначені основні існуючі загрози безпеці інформації для смартфонів з ОС Android та окреслені основні рекомендації щодо протидії цим загрозам.

Мороз А.А. (ВІТІ)
Нерознак Є.І. (ВІТІ)

РЕАЛІЗАЦІЯ ВІДДАЛЕНОГО АДМІНІСТРУВАННЯ МЕРЕЖЕВОГО ТА СЕРВЕРНОГО ОБЛАДНАННЯ

Актуальність проведення дослідження

На сьогоднішній день актуальність даної роботи повязана з тим що реалізація локального адміністрування серверного та мережевого обладнання не завжди можлива або зручна. Часто складається ситуація, коли об'єкти адміністрування географічно віддалені один від одного або перебувають поза межами одного приміщення. У цьому випадку важливо організувати роботу таким чином, щоб, перебуваючи на віддалі від мережевого та серверного обладнання, адміністратори мали можливість підключатися віддалено. Для забезпечення даного методу адміністрування при відсутності можливості локального підключення, використовуються засоби та протоколи віддаленого доступу.

Метою зазначеного дослідження є розробка та реалізація програмного інтерфейсу для віддаленого адміністрування мережевого та серверного обладнання.

Для реалізації даного програмного забезпечення потрібен певний набір інструментів прикладного програмування, які надають платформу і середовище для розробки програмного забезпечення віддаленого адміністрування через Aplication Programming Interface (далі API).

API визначає набір правил для взаємодії однієї програми з іншою. Більшість API мають належну документацію, яка також визначає характер і структуру відповіді, яку вони відправляють, коли реалізовується запит, а також вказують необхідну інформацію, яку повинен надати клієнт для успішного запиту до API.

Також важливим аспектом є робота з архітектурою Representational State Transfer (далі REST), яка являє собою стиль архітектури API для розподілених систем. REST визначає, як дані надаються клієнту в зручному для нього форматі. Обмін даними відбувається у форматі JSON (JavaScript Object Notation) або XML (Extensible Markup Language) за допомогою стеку протоколів TCP/IP (Transmission Control Protocol/Internet Protocol), який описує взаємодію великої кількості клієнтів, підключених до мережі.

TCP/IP забезпечує наскрізний зв'язок, який визначає: як саме дані обмінюються через мережу, як дані розбиваються на пакети, як пакети кодуються, адресуються, маршрутизуються і приймаються в місці призначення.

Таким чином, досягнення даної мети можливе шляхом розробки програмного додатку на скриптовій мові програмування PHP (Hypertext Preprocessor), яка генерує HTML-сторінки на стороні веб-сервера та передає на сторону клієнта у вигляді HTML-коду, що в свою чергу забезпечить візуалізацію.

В свою чергу, додаток програмних компонентів візуалізує розміщення мережевого та серверного обладнання в монтажній стійці для зменшення часу пошуку конкретного обладнання з метою його адміністрування. Надає можливість віддалено налаштувати мережеве та серверне обладнання та забезпечує підключення по захищеному протоколу SSH (Secure SHell).

Висновок

Проаналізувавши засоби для розробки програмного додатку було створено та реалізовано програмний web-інтерфейс, який надає можливості віддалено адмініструвати мережеве та серверне обладнання.

Програмний додаток не потребує додаткової інсталізації так як процес підключення та налаштування відбувається за допомогою веб-браузера.

Розробка програмного інтерфейсу є перспективною і актуальною так як вона дозволяє виконувати завдання пов'язані з роботою з мережевим обладнанням та сервером, при цьому вона не вимагає вкладання фінансів що робить її доступною.

к.т.н. Нагорнюк О.А. (ЖВІ)
к.т.н. Колос Ю.О. (ЖВІ)

ВПЛИВ КОНСТРУКТИВНИХ РІШЕНЬ КОМПОНУВАННЯ ТА ПОХИБОК У ВИГОТОВЛЕННІ ЕЛЕМЕНТІВ ШИРОКОСМУГОВОЇ РУПОРНОЇ АНТЕНИ НА ЇЇ ТЕХНІЧНІ ХАРАКТЕРИСТИКИ

Сучасними тенденціями розвитку радіотехнічних та телекомунікаційних засобів є розширення діапазону їх робочих частот та застосування широкосмугових радіосигналів із складними видами модуляції. Для приймання та передавання таких сигналів необхідно використовувати широкосмугові антени із високим коефіцієнтом перекриття за частотою та доброю узгодженістю із лінією живлення. Вказані технічні характеристики забезпечують рупорні антени із складною формою поперечного перерізу. В літературі представлено ряд методик розрахунку конструктивних розмірів та параметрів таких видів антен, а також результатів їх оптимізації з використанням спеціалізованого програмного забезпечення CST STUDIO SUITE, ALTAIR FEKO, ANSOFT HFSS та інших. Запропоновані конструкції рупорних антен із складною формою поперечного перерізу працездатні в діапазоні від 0,7 до 30 ГГц та мають коефіцієнт стоячої хвилі за напругою (КСХН) менше 2. Однак в наявних у відкритому доступі роботах мало уваги приділяється дослідженню впливу конструктивних рішень компонування та похибок в виготовленні елементів широкосмугової рупорної антени на її технічні характеристики.

В доповіді представлено результати дослідження найбільш розповсюджених варіантів практичного виготовлення двогребеневої рупорної антени, які відрізняються способами кріплення елементів: болтове з’єднання, заклепки, пайка та їх комбінування. Крім того проаналізовано вплив неточностей в виготовленні окремих елементів антени (похибки в геометричних розмірах хвилеводу та розкриву рупора, похибки розміщення провідника живлення, відмінності діелектричної проникності ізолюючого матеріалу від розрахованої та інші) та в з’єднанні елементів антени між собою (ширина щілин між пластинами розкриву рупора, відстань між діелектриком провідника живлення та металевою пластиною хвилеводу, відстань між гребнями в точці збудження та інші) на основні характеристики антени (КСХН, коефіцієнт підсилення (КП), діаграму спрямованості, вхідний опір). Дослідження проводились із використанням програмного середовища моделювання та оптимізації тривимірних електромагнітних систем CST STUDIO SUITE.

Встановлено, що при однаковій точності виготовлення складових елементів широкосмугової рупорної антени розглянуті варіанти компонування забезпечують близькі за значенням технічні характеристики. Дослідження похибок виготовлення елементів антени показали, що найбільший вплив на характеристики антени мають розміри хвилеводу, розміри гребнів, місце розміщення, діаметр та довжина провідника живлення, діелектричні характеристики ізолюючого матеріалу. Так зміщення провідника живлення вздовж широкої стінки хвилеводу на 0,5 мм та похибка встановлення гребнів 0,2 мм призводять до збільшення КСХН в два рази. Ширина щілин між поверхнями розкриву рупора до 0,4 мм суттєво не впливає на його КСХН та КП, однак при більшому її значенні виникають резонансні явища і максимальне значення КСХН перевищує 4, а середнє значення КП падає. Якщо вказані щілини заповнити металом, наприклад оловом, то резонансні частоти зникають, а значення КСХН та КП практично не змінюються

Відповідно до проведених результатів моделювання виготовлено макет широкосмугової рупорної антени з діапазоном робочих частот від 2–15 ГГц за однією із досліджених схем компонування. Виміряні технічні характеристики макету відповідають отриманим в процесі моделювання програмним засобом CST STUDIO SUITE, що підтверджує достовірність результатів.

Назаренко І.М. (ВІТІ)
Троцько О.О. (ВІТІ)

МОДЕЛЬ СИСТЕМИ РЕАГУВАННЯ НА ІНЦИДЕНТИ В МЕРЕЖІ НА ОСНОВІ ПРОГРАМНОГО СТЕКУ ELK

Проблема безпеки та цілісності данних завжи є актуальною у всіх сверах життя, особливо у сфері захисту країни. Є багато способів слідкувати за станом мережі або серверів, наприклад, перегляд системних журналів, таблиць маршрутизації, записів мережевих екранів. Найбільш раціональним методом є перегляд файлів логування. Пристрій сам фіксує помилки в конфігурації або факти порушення політики безпеки та записує їх у файл, адміністратору лишається лише переглянути та вжити заходів щодо усунення несправностей. Для підтримки стабільної роботи мережевих пристроїв та серверів звичайного перегляду лог-файлів недостатньо, потрібно аналізувати , систематизувати всі події стосовно помилок в роботі пристроїв. Результатом аналізу є події які співвідностяться до інцидентів. На основі аналізу можливо створити певні правила які будуть реагувати на інциденти. Одним їз варіантів вирішення цієї проблеми є встановлення сервісів які контролюють стан мережі, серверів та цілісність данних. На данний момент існує чимало додатків за допомого яких можливо виявляти вторгнення *IDS* (*Intrusion Detection System*) або реагувати на інциденти *IPS (Intrusion Prevention System)*, але вони не надають всіх потрібних можливостей. Вони не дозволяють зберігати та проводити детальний аналіз мережевих інцидентів. Одним із варіантів рішення цієї проблеми є впровадження *SIEM (Security information and event management)* системи. Поняття *SIEM* у комп'ютерній безпеці є програмними продуктами, які об'єднують управління інформаційною безпекою *SIM* (*Security information management*) та управління подіями безпеки *SEM (Security event management).*У якості джерел повідомлень для *SIEM* можливо використовувати: антивірусні програми, журнали повідомлень операційних систем, між мережеві єкрани, *IDS/IPS* системи. Використання *SIEM* дозволяє аналізувати події в режимі реального часу, та автоматично реагувати на інциденти, виконувати аналіз данних та зберігати інформацію про результати роботи. Іноді звичайного реагування на порушення політики безпеки не вистачає. Потрібне негайне втручання системного адміністратора. Тому з'являється необхідність використання засобу для сповіщення за допомогою відправки повідомлень через спеціальні месенджери або через електронну пошту. Одним із компонентів *SIEM* системи є модуль сповіщення. Крім того *SIEM* забезпечує корелячію подій, а саме визначає взаємозв'язки між подіями. Складовою будь-якої *SIEM* системи є елемент зберігання інформації про інциденти. З цією функцією в повному обсязі справляється стек *ELK*. Це три програмних продукта: *Elasticsearch, Logstash, Kibana.* В якості середовища для зберігання використовується *Elasticsearch. Kibana* забезпечує динамічне відображення інформації з *Elasticsearch. Logstash* відігрує роль конвеєра для інформації від мережевих пристроїв або серверів, завдяки якому інформація приводиться до зручного вигляду та формату. Завдяки використанню *SIEM* системи підвищюється рівень захисту інформаційних систем від зовнішніх загроз. А за рахунок оперативного реагування на інциденти інформаційної безпеки підвищується рівень захисту від кібер-атак. З'являється можливість отримання даних для процесів аналізу та керування ризиками інформаційної безпеки. Знижуються витрати за рахунок автоматизації процесів обробки та керування інцидентами від різних джерел. Метою подальших досліджень є створення *SIEM* системи на основі стеку *ELK* для подальшого її використання в ЗСУ.

Рис. 1 Модель *SIEM* системи

Нерознак Є.І. (ВІТІ)
Кравченко А.О. (в/ч А2724)
д.т.н. Сова О.Я. (ВІТІ)

АНАЛІЗ МЕТОДОЛОГІЙ, АРХІТЕКТУРНИХ РІШЕНЬ ТА ІНСТРУМЕНТАРІЮ РОЗРОБКИ ІНФОРМАЦІЙНИХ СИСТЕМ ТА АСУ МЕРЕЖЕВИМИ ІНФРАСТРУКТУРАМИ

На сьогодні, у великих організаціях, у тому числі Збройних силах України, використовується велика кількість мережевих пристроїв, які потрібно налаштовувати, оновлювати та моніторити їх працездатність. Обслуговування такого парку обладнання є досить складним процесом, який вимагає багато сил, засобів та часу. Вирішення даних питань можливе шляхом автоматизації вищезазначених процесів управління мережевими інфраструктурами.

У даний час існує значна кількість підходів до організації процесу розробки різного роду інформаційних систем та автоматизованих систем управління (АСУ) як на рівні взаємодії фахівців, які залучаються до даного процесу, так і на рівні взаємодії технічних та програмних засобів, які будуть складати основу майбутньої системи чи АСУ. У зв'язку з цим, ***метою даного дослідження*** є проведення аналізу існуючих методологічних підходів, архітектурних рішень та інструментарію розробки систем автоматизації управління мережевими інфраструктурами. Серед великої кількості методологічних підходів щодо організації розробки, впровадження та управління інформаційними системами, одними з найпопулярніших є ITIL, *Agile*, *DevOps*. Розглянемо їх детальніше.

ITIL (*Information Technology Infrastructure Library*, бібліотека інфраструктури інформаційних технологій) – це методологія управління, налагодження і безперервного поліпшення бізнес-процесів, пов'язаних з використанням інформаційних технологій як з погляду користувачів, так і з погляду організації, що надає послуги у сфері інформаційних технологій. Ця методологія допомагає забезпечити стабільний і передбачуваний розвиток інформаційної системи, описуючи базові процеси, що забезпечують підтримку й надання IT сервісів, які складають основу життєвого циклу послуги.

Agile – це методологія, яка містить в собі сукупність гнучких підходів до розробки програмних продуктів, які базуються на ітеративній розробці, в якій вимоги та розв'язки еволюціонують через співпрацю між багатофункціональними командами здатними до самоорганізації. Ця методологія націлена на мінімізацію ризиків, шляхом зведення розробки до серії коротких циклів, що мають назву ітерацій, які зазвичай тривають один-два тижні. Кожна ітерація сама по собі виглядає як програмний проект в мініатюрі, і включає всі завдання, необхідні для видачі мінімального приросту за функціональністю: планування, аналіз вимог, проектування, кодування, тестування і документування. Хоча окрема ітерація, як правило, недостатня для випуску нової версії продукту, мається на увазі те, що гнучкий програмний проект готовий до випуску наприкінці кожної ітерації. Після закінчення кожної ітерації, команда виконує переоцінку пріоритетів розробки.

Ітеративна та інкрементна розробка являє собою ядро циклічного процесу розробки програмного забезпечення, який починається з планування і закінчується впровадженням готового програмного забезпечення з циклічними взаємодіями між цими етапами. При цьому, гнучкість підходів полягає в тому, що замовник формує вимоги поступово, в залежності від змін зовнішніх чинників, які впливають на вимоги до кінцевого програмного продукту, що може відбуватися навіть на пізніх стадіях розробки.

DevOps (***„development"*** – розробка***, „operations"*** – експлуатація) – новітня технологія (методологія) яка на відміну від попередніх, які зосереджують увагу на процесах розробки програмного забезпечення, зосереджується на організації тісної взаємодії самих фахівців з розробки та експлуатації програмного забезпечення.

В кінцевому результаті, системи автоматизації збірки і випуску програмного забезпечення повинні бути доступні всім розробникам в будь-якій групі, і у розробників повинен бути контроль над всіма групами, а інформаційно-технологічна інфраструктура повинна бути більш орієнтована на додатках. Іншими словами, ця методологія фокусується на об'єднанні окремих людей, груп чи відділів розробки та експлуатації з метою сприяння швидкому досягненню спільних цілей, але при цьому не визначається тільки певним набором інструментів, а лише налічує у своєму контексті певну структуру, яка базується на взаємній співпраці окремих фахівців, їх процесі формування взаємовідносин між собою, інструментах розробки та впровадження, та масштабуванні. Цільовою задачею цієї методології є створення погодженого процесу розробки і доставки програмного забезпечення та експлуатації, і як правило ці задачі вирішуються завдяки застосуванню автоматичних засобів. Зазначені вище методології спрямовані на організацію процесів щодо створення, розвитку та безперервного удосконалення IT інфраструктур, які практично реалізовуються шляхом застосування існуючих архітектурних рішень, зокрема:

Інфраструктура як сервіс (IaaS) – це модель надання обчислювальних послуг, відповідно до якої постачальник послуг IaaS забезпечує доступ замовнику (користувачеві) до певних обчислювальних ресурсів та відповідає за технічний стан наданої інфраструктури.

Характерні риси IaaS:

– масштабування інфраструктури відбувається в реальному часі, в залежності від потреб замовника (користувача);

– замовник не витрачає власні ресурси на обслуговування апаратного забезпечення;

– питання доступу, безпеки та відмовостійкості інфраструктури вирішує виконавець.

Платформа як сервіс (PaaS) – це модель надання обчислювальних послуг, відповідно до якої постачальник послуг PaaS забезпечує доступ замовнику (користувачеві) до налаштованої та працездатної платформи (мережеве та серверне обладнання, системи віртуалізації, віртуальні підмережі та фаєрволи, операційні системи, системи збереження та СУБД) для подальшого розгортання додатків замовника (користувача).

На відміну від IaaS – постачальник послуг PaaS надає можливість вибору преналаштованих операційних систем (систем збереження, баз даних та ін. в залежності від потреб замовника) з наявних у нього, та бере на себе зобов'язання щодо забезпечення їх повного життєвого циклу. Характерною рисою PaaS, окрім тих які були зазначені для IaaS, є наявність готових інфраструктурних сервісів (операційні системи, системи збереження та СУБД) та можливість їх конфігурування під потреби замовника (користувача).

Програмне забезпечення як сервіс (SaaS) – це модель надання послуг, в рамках якої постачальник розміщує власний додаток у хмарному середовищі, та надає доступ до нього користувачам через мережу інтернет.

Основні функції:

– користувачам не потрібно встановлювати або оновлювати ПО, а також керувати ним, це роблять постачальники SaaS;

– дані в хмарі захищені: збій обладнання не призводить до втрати даних;

– програмне забезпечення є доступним майже з будь-якого пристрою, підключеного до мережі Інтернет, і практично в будь-якій точці світу.

Робоче місце як сервіс (DaaS) – це модель надання послуг, в рамках якої постачальник послуг DaaS надає повністю готове до роботи стандартизоване віртуальне робоче місце, яке кожен користувач (замовник) має можливість додатково налаштовувати для вирішення своїх конкретних задач, таким чином користувач отримує доступ не до окремої програми, а до необхідного для повноцінної роботи програмному комплексу. Такий підхід поєднує в собі відразу два архітектурних рішення як „програмне забезпечення як сервіс (SaaS) " та „платформа як сервіс (PaaS)".

Мережа як сервіс (NaaS) – це модель застосування інфраструктури як концепції коду для всього мережевого домену включаючи центри обробки даних, глобальні та локальні мережі, хмарні середовища та інші. Реалізація цього підходу являється частиною більш

широкого застосування методології NetDevOps в організації і змінює уявлення про архітектуру і роботу мережі, інструментарій і технології, які використовуються для створення і управління мережевими конфігураціями. У процесі розвитку наведених архітектурних рішень, процеси розгортання та управління інфраструктурою, платформою, програмним забезпеченням, мережею та ін., набули певної трансформації, яка пов'язана із можливістю автоматизованого конфігурування даними архітектурними рішеннями за допомогою програмного коду (набору скриптів), що сприяло розвитку нових архітектурних рішень, зокрема таких як: „Інфраструктура як код (IaaC) ", „Платформа як код (PaaC) ", „Програмне забезпечення як код (SaaC) ", „Архітектура як код (AaaC) " „Мережа як код (NaaC)". Як було зазначено вище, одним із завдань наведених методологій управління інформаційними системами є організація спільної роботи над проектами. На практиці це потребує наявності ефективного інструменту контролю версій (Git, GitLAB, GitHUB), вихідних кодів (конфігурацій мережевого та серверного обладнання (Ansible, Terraform, Puppet, Vagrant)) та інструменту управління процесом постановки та контролю виконання завдань (Scrum, Kanban та інші). Розглянемо детальніше найбільш використовувані з них.

Системи управління конфігураціями мережевого та серверного обладнання:

Ansible – це інструмент з відкритим вихідним кодом для управління конфігураціями з використанням декларативної мови розмітки для опису конфігурацій, розроблений компанією RedHat на мові програмування Phyton, яка використовується для розгортання та налаштування програмного забезпечення. До особливостей даної системи відноситься підтримка розпаралелювання завдань, відсутність необхідності встановлення на віддалені системи спеціальних програм-агентів, так як всі операції ініціюються централізовано по захищеному протоколу підключення SSH. Важливою властивістю даного інструменту є „індемпатентність", тобто він порівнює поточний стан системи з новоствореним сценарієм конфігурації для запобігання виконання повторних завдань.

Terraform – це інструмент з відкритим вихідним кодом для розробки та управління конфігураціями хмарною інфраструктурою розроблений корпорацією HashiCorp на мові програмування Go та використовує мову конфігурації високого рівня HashiCorp Configuration Language (HCL), також підтримує „оркестрацію" за допомогою якої можна легко створювати таку інфраструктуру як код (Infrastructure as a code). Даний інструмент відслідковує поточний стан системи, але на відміну від Ansible, при зміні конфігурацій його потрібно перезапускати вручну.

Puppet – це багатоплатформенний клієнт-серверний додаток, який дозволяє централізовано керувати конфігурацією операційних систем та програм, втановлених на кількох комп'ютерах, та надає можливість легко налаштовувати і в подальшому швидко керувати кожною мережею на базі будь-якої операційної системи сімейства Linux, Microsoft Windows та MAC OS.

Vagrant – це відкритий інструментарій для спрощення створення, встановлення та керування образами віртуальних машин при вирішенні завдань пов'язаних з розробкою та тестування проектів з використанням різних систем віртуалізації, який дозволяє згенерувати готове до роботи середовище розробки із заданими параметрами та компонентами використовуючи єдиний конфігураційний файл.

Системи контролю версій:

Git – розподілена система керування версіями, спроектована як набір програм спеціально розроблених із врахуванням їх використання в сценаріях. Це дозволяє зручно створювати спеціалізовані системи контролю версій на базі Git. Також ця система підтримує швидке розділення и злиття версій та включає в себе інструменти візуалізації та навігації по історії розробки.

GitHUB – це веб-сервіс для хостингу IT-проектів та їх спільної розробки, в основі якого лежить система контролю версій Git. Крім розміщення програмного коду, розробники мають змогу спілкуватись, коментувати зміни один одного, об'єднувати свої репозиторії.

Крім того цей сервіс надає зручний інтерфейс для цього, та має можливість відображти вклад у спільну розробку кожного розробника у вигляді „дерева”.

Системи управління процесом постановки та контролю виконання завдань:

Kanban – інструмент візуалізації роботи команди розробників, який відображає стратегію оптимізації потоку поставки продукту через процеси, які використовують візуальну систему, яка має обмеження незавершеної роботи та досягнення максимальної ефективності потоку. За допомогою даного інструменту команди зосереджуються на скороченні часу, необхідного на те, щоб проект пройшов від початку до кінця, використовуючи дошку Kanban і постійно вдосконалюючи свій потік роботи.

Scrum – це інструмент візуалізації роботи команди розробників, який відображає структуру в рамках якої розробники можуть вирішувати складні адаптивні проблеми та дозволяє організувати та відображати процес розробки програмного забезпечення через встановлені інтервали, що називаються „спринтами”, цим самим за його допомогою надається можливість прояснити відносну ефективність керування продуктом та методів роботи для того щоб постійно покращувати продукт, роботу команди та робоче середовище.

Основна різниця між даними інструментами полягає саме у довжині ітерацій, тобто основу Scrum складають короткі ітерації або „спринти”, як правило 2-3 тижні, перед початком ітерації команда розробників формує список виправлень на ітерацію, далі починається „спринт”. Після завершення „спринта” виконані виправлення переносяться в продуктивну систему, а не виконані – переносяться на інший „спринт», як правило, виправлення, які виконуються під час виконання „спринту”, не змінюються, кажучи іншими словами: які задачі були поставлені на початку „спринта”, повинні обов’язково виконатись до його завершення. Щодо інструменту Kanban, то він надає більше гнучкості, тобто під час процесу розробки є можливість вносити зміни незалежно від часових рамок роботи команди розробників. На сьогодні ефективне управління інформаційними технологіями передбачає все більше використання технологій віртуалізації, зокрема серверного обладнання, які дозволяють ефективно управляти серверними ресурсами і особливо важливими при використанні технологій віртуалізації є підвищення доступності інфраструктур та можливість проводити зміни апаратних платформ без обмеження безперервності.

Наступним етапом розвитку технологій віртуалізації є технологія контейнеризації, яка являє собою ізоляцію ресурсів на рівні операційної системи та дозволяє завантажувати додатки з мінімальним використанням системних та апаратних ресурсів. Для практичної реалізації вищезазначеної технології використовуються наступні програмні інструменти: Docker, LXC, LXD та ін. Розглянемо їх детальніше.

Docker – це інструмент з відкритим кодом, який дозволяє розробникам, системним адміністраторам та іншим фахівцям розгортати додатки в контейнерах, для запуску на цільовій операційній системі. Ключовою перевагою цього інструменту є те, що він дозволяє користувачам здійснювати інкапсуляцію додатка зі всіма його залежностями в стандартизований модуль для розробки. На відміну від віртуальних машин, контейнери не створюють додаткового навантаження, саме тому за їх допомогою можна використовувати систему та ресурси більш ефективніше.

LXC (Linux Containers) – це інтерфейс в просторі користувача, який дозволяє легко створювати та керувати системними або прикладними контейнерами. LXC використовує наступні функції ядра для того, щоб здійснити контейнеризацію: простору імен ядр; AppArmor та SELinux профілі; умови Seccomp; можливості ядра; контрольні групи (групи управління).

Ціллю LXC являється створення середовища максимально близького до стандартної інсталяції Linux, але необхідної потреби в окремому ядрі.

LXD – це гіпервізор контейнерів, який базується на LXC котрий складається з трьох компонентів: системного демона (lxd), клієнта командного рядка (lxc) та плагіна OpenStack Nova. Ключовими особливостями LXD являються:

– безпека (непривілейовані контейнери, обмеження ресурсів, тощо);

– масштабування (від контейнерів на одному пристрої до тисячі обчислювальних вузлів);

– інтуїтивно зрозумілий (простий у використанні, зрозумілий API, керування з командного рядка);

– базується на образах (відсутність шаблонів розповсюдження);

– жива міграція.

Основна відмінність зазначених інструментів полягає в тому, що Docker спеціалізується на розгортанні додатків, а LXC (LXD) спеціалізується на розгортанні віртуальних машин на базі операційних систем сімейства Linux. Функції систем управління конфігураціями потребують налаштування та виконання сценаріїв налаштувань, які ініціюються в ручному режимі, що є трудомістким процесом, який може містити помилки, пов'язані з людським чинником. Для запобігання вищезазначеного пропонується використання інструментів безперервної інтеграції програмного забезпечення, зокрема, Jenkins, TeamCity та ін.

Jenkins – це інструмент з відкритим вихідним кодом для безперервної інтеграції програмного забезпечення, який допомагає автоматизувати частину процесу розробки програмного забезпечення, яка в свою чергу не потребує безпосередньої участі людини у процесі безперервної інтеграції, та розширює технічні можливості команд розробників у процесі неперервної доставки програмного продукту.

TeamCity – це інструмент з відкритим вихідним кодом для безперервної інтеграції програмного забезпечення, який підтримує системи контролю версій, аутентифікації та тестування, при чому легко масшабується та має наступні ключові можливості:

– миттєве оповіщення про помилки версії;

– підтримка Java та .NET проектів;

– підтримка Ruby та XCode проектів;

– ієрархічна структура проектів;

– керування фермою білд-агентів;

– інтеграція з системами контролю версій та ін.

Висновки

Таким чином, на сьогодні існує низка методологій щодо організації розробки, супроводження та управління інформаційними системами та АСУ мережевими інфраструктурами, кожна з яких призначена для поліпшення та підвищення ефективності елементів зазначених систем протягом всього життєвого циклу. Разом з тим, кожна з цих методологій не є стандартом чи панацеєю, здатною вирішити всі проблеми, що виникають в процесі розробки будь-якої системи. Вибір тієї чи іншої методології залежить від множини чинників, які визначаються умовами середовища, в якому перебуває та чи інша організація, та завданнями, які стоять перед нею. У свою чергу, вибрана методологія та умови середовища будуть впливати на архітектурні рішення щодо розробки та використання майбутніх систем. Практична реалізація зазначених методологій та архітектурних рішень здійснюється з використанням множини програмних інструментів, які в загальному можна поділити на комерційні та некомерційні (OpenSource). Проаналізовані в ході дослідження інструменти відносяться до програмних додатків з відкритим вихідним кодом та знаходяться у вільному доступі, що дає змогу їх апробації та модифікації, в залежності від потреб. Правильна комбінація цих інструментів дозволяє розробляти та використовувати гнучкі інформаційні системи та автоматизовані системи управління мережевими інфраструктурами. Крім того, використання OpenSource-додатків схвалюється методологією FMN (*Federated Mission Network*), яка спрямована на забезпечення оперативної сумісності, обміну інформацією та розвідувальними даними під час спільних операцій держав-членів НАТО та країн-партнерів.

к.т.н. Нестеренко М.М. (ВІТІ)
Баюра А.І. (ВІТІ)

ПРОГРАМНИЙ МОДУЛЬ АДАПТИВНОЇ ПОБУДОВИ МОДЕЛІ ДЛЯ *3D* ДРУКУ ЗА ТЕХНЛОГІЄЮ *FDM*

На сьогоднішній день одним із пріоритетних завдань як в промисловості так і у військовому оборонному комплексі є мінімізація затрат при виробництві запчастин та готових компонентів. Одним із перспективних напрямків вирішення задачі мінімізації затрат ресурсів при виготовленні різного роду виробів можуть стати технології *3D* друку. При чому, переваги використання сучасних *3D* принтерів очевидні: зниження собівартості та скорочення термінів виготовлення прототипів (серійне виробництво), моделювання елементів будь-якої форми і складності, швидкість та висока точність виготовлення, можливість використання різнорідних матеріалів. У поєднанні з потужними сучасними програмними інструментами проектування, такий тип виробництва дозволяє створювати конструкції будь-якої складності. Швидке виробництво кінцевого продукту, цифрова обробка, і як наслідок висока точність виготовлення, не викликають сумніву щодо актуальності технологій *3D*-друку.

В даний час існує більш ніж 100 зареєстрованих методів *3D* друку, таких матеріалів як полімери та метали. Необхідно відмітити, що кожна компанія, яка займається виробництвом *3D* принтерів, намагається зареєструвати свій власний метод друку та зареєструвати як об’єкт інтелектуальної власності. Проведений аналіз показав, що методи відрізняються лише назвою, а не технологією. Таким чином, різні технології в загальній складності налічують близько 15 методів *3D* друку.

Виробничий цикл починається з обробки тривимірної цифрової моделі. Модель в форматі *STL (Standard Template Library)* ділиться на шари та орієнтується найбільш оптимальним чином в залежності від обраної технології друку. Для розробки архітектури *3D* принтера було обрано технологію друку *Fused deposition modeling (FDM)* – моделювання методом пошарового наплавлення (технологія адитивного виробництва). *FDM* застосовується для створення тривимірних моделей, макетів, виробів до яких не висуваються жорсткі вимоги до якості поверхні і точності виготовлення.

При виготовленні деталей з пластика, дана технологія дозволить швидко створити прототип деталі із можливістю повторного тестування з послідовною, покроковою модернізацією об’єкта. Для того, щоб друкувати на *3D*-принтері, необхідно створити *3D*-модель в форматах *.STL, .OBJ, .AMF, .GCO, .G, .NC*. Це можливо при використанні програми тривимірного моделювання і проектування, або завантажити з бібліотек, представлених в мережі інтернет.

Щоб здійснити пошарове розрізання моделі на шари, можемо використати програми-слайсери: *Slic3r, KISSliser, Cura* і інші. У керуючу програму *Repetier-Host* вбудований слайсер, але можна використовувати і сторонні програмні продукти.

В результаті проведеної роботи було розроблена архітектура *3D* принтера за технологією *FDM*, в якості мікроконтролера була використана платформа *Arduino Mega*, а також був адаптований *sketch* (скетч) для налаштування та взаємодії елементів та шасі принтера. Великий плюс *FDM*-технології полягає: у швидкому розгортанні виробництва навіть у польових умовах; використання в якості недорогої альтернативи стандартним методам при створенні дрібносерійних партій; низька собівартість готової друкованої деталі. В зв’яку з цим дана технологія знайшла широке застосування для створення комплектуючих безпілотних літальних апаратів, робототехніки на наземному шасі, а також для елементів для протезування та озброєнням.

В подальшому планується розробити програмний модуль для адаптивної побудови цифрової моделі для *3D* друку за технологією *FDM*.

к.т.н. Нестеренко М. М. (ВІТІ)
Богуцький В. В. (ВІТІ)

ВІРТУАЛЬНО-ТРЕНАЖЕРНИЙ КОМПЛЕКС „ТЕЛЕКОМУНІКАЦІЙНИЙ КОМПЛЕКТ ТИП-1” НА ОСНОВІ ПРОГРАМНОГО СЕРЕДОВИЩА *UNITY3D*

Сучасні тенденції розвитку 3D моделювання та використання програмних інтерактивних систем обумовлюють їх широке застосування для створення тренажерних систем для подальшого використання в організації навчального процесу. Особливо гостро дане питання постає при обмеженій кількості новітнього обладнання та стислих термінах для опанування налагодження та роботи на ньому.

Для побудови сучасних тренажерних систем використовується різне програмне забезпечення, яке називають *game engines* (*GE*), дослівно – ігрові рушії. У *GE* (ігрових рушіях) реалізовані механізми роботи з *2D* або *3D* графікою, що застосовується для створення тренажерів різних типів.

За результатами аналізу *GE* рушіїв для реалізації поставленого завдання було обрано середовище розробки *Unity3D*. Дане програмне забезпечення дозволяє у повному обсязі реалізувати функції імітації (емуляції) налаштування мережевого обладнання та має ряд переваг над своїми конкурентами, а саме: безкоштовне використання у некомерційних цілях; простий користувацький інтерфейс; використання скриптів на мові *C#* для побудови програмної логіки; низький рівень використання ресурсів пристрою, на якому запущений додаток; кросплатформність; використання засобів роботи з анімаціями та *3D* моделями, що дозволяє створювати інтерактивність та наочність роботи із віртуальним тренажером.

Проаналізувавши основні тактико-технічні характеристики обладнання, порядок та термін виконання основних нормативів, було створено віртуальний тренажер „Телекомунікаційний комплекс Тип-1” на базі рушія *Unity3D* (рис. 1).

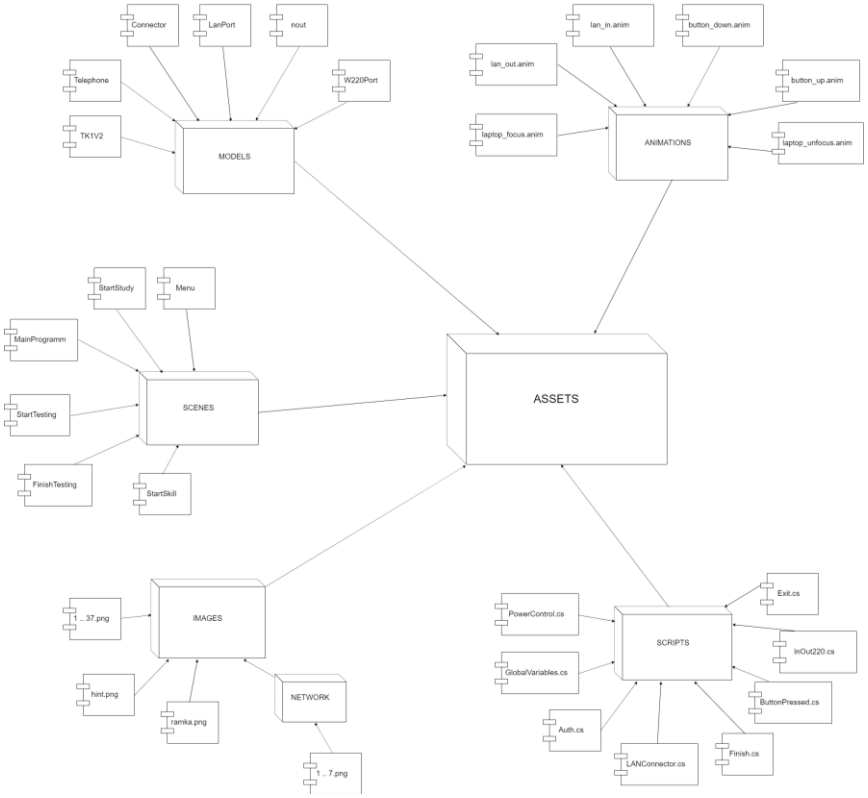


Рис. 1. Структурна схема тренажера

При розробці було використано переваги рушія, а саме: математично-фізична модель; робота з анімаціями та *3D* графікою. Також для реалізації симуляції налаштування пристрою було створено скрипти на мові C# та розроблені сценарії для різних режимів удосконалення своїх практичних навичок, а саме:

– режим навчання – у даному режимі реалізовано поетапне налаштування пристрою із спливаючими підказками, для того щоб користувач, який вперше знайомиться із пристроєм, мав поняття його призначення. Режим не використовує складну модель, тому що його реалізація не потребує розрахунків та перевірки налаштованих опцій мережевого обладнання.

– режим тестування – у даному режимі відбувається тренування з налаштування пристрою. Реалізація даного сценарію важча з причини реалізації функції перевірки налаштування певних опцій, наприклад: підключення живлення, налаштування *IP*-адреси та інші. Після того, як користувач проходить тест, програма визначає помилки, які виникли під час налаштування.

– здача іспиту – у даному режимі реалізована математична модель розрахунку часу налаштування (відлік часу починається з моменту введення індивідуальних даних користувача і завершується після натискання користувачем відповідної кнопки закінчення налаштування). Після закінчення проходження іспиту викладач може відслідкувати результати здачі нормативів військовослужбовцями, які проходили даний іспит. Для збереження та оброблення статистики результатів було використано базу даних *MySQL*, яка створена на базі *Xampp* серверу. Для керування базою даних із середовища віртуального тренажера використано бібліотеку роботи з базою даних *MySqlConnector*;

Рис. 2. Віртуальний тренажер „Телекомунікаційний комплект Тип – 1”

В подальшому планується створення тренажерної системи на основі розробленого тренажера „Телекомунікаційний комплект Тип – 1” з наступними функціями:

– одночасне налаштування декількох комплектів та подальшої перевірки зв’язку між ними у випадку коректного налаштування віртуального мережевого обладнання;

– налаштування комплекту за допомогою емуляції роботи терміналу та елементів управління ТК – 1;

– створення підсистеми контролю успішності з можливістю віддаленого доступу викладача до бази даних отриманих результатів.

Таким чином, створення тренажерної системи на основі тренажера „Телекомунікаційний комплект Тип – 1” дозволить насамперед підвищити гнучкість налаштування обладнання, збільшити кількість доступних нормативів та підвищити ефективність навчання військовослужбовців в цілому.

к.т.н. Нестеренко М.М. (ВІТІ)
Ткаченко Б.О. (ВІТІ)

ПРОГРАМНИЙ МОДУЛЬ КОНФІГУРУВАННЯ ТА УПРАВЛІННЯ СЕГМЕНТОМ ВІРТУАЛЬНОЇ МЕРЕЖІ SDN

На сьогоднішній день однією із перспективних мережевих технологій є *Software-defined networking* (*SDN*). *SDN* це програмно-конфігурована мережа яка використовує протокол *OpenFlow* для обміну інформації між активними мережевими елементами. Концепція програмно-конфігуровних мереж має великий потенціал і допомагає вирішити проблеми, що зустрічаються в класичних підходах щодо побудови сучасних інфокомунікаційних мереж: зменшити часові витрати на розгортання мережі за рахунок використання більш простих мережевих пристроїв; підвищити контроль за мережею, за рахунок чіткого відокремлення рівня пересилки даних та рівня управління.

Для побудови та дослідження даної технології можна використовувати емулятор комп'ютерної мережі *mininet.* Який в свою чергу, дозволяє побудувати сегмент віртуальної *SDN* мережі на базі протоколу *OpenFlow* та має вбудований контролер. Однак вбудований контролер має ряд недоліків, які роблять його непридатним для проведення експериментів та гнучкого налаштування.

На даний момент існує більш як 20 реалізацій мережевих ОС для програмно – конфігурованих мереж: *NOX, POX, Beacon, Maestro, Trema, BigSwitch, FloodLight* та інші.

Для визначення ефективності різних контролерів проводять тести. *Cbench* є найбільш часто використовуваним інструментом тестування для контролерів *SDN*. За результатами дослідження, контролери, написані на мові C / C ++, показали найвищу продуктивність (*Mul, Libfluid_msg*), поступаються в продуктивності контролерам, написані на *Java*, такі як *Beacon, Iris і Maestro*.

Було використано контролер від фірми *Aruba*, який дозволяє розробляти специфічні правила для контролю та управління мережевим трафіком. В результаті проведеного аналізу функціональних можливостей засобів віртуалізації, емуляторів комп'ютерних мереж та операційних систем контролерів було розроблено віртуальний сегмент SDN мережі (рис. 1).

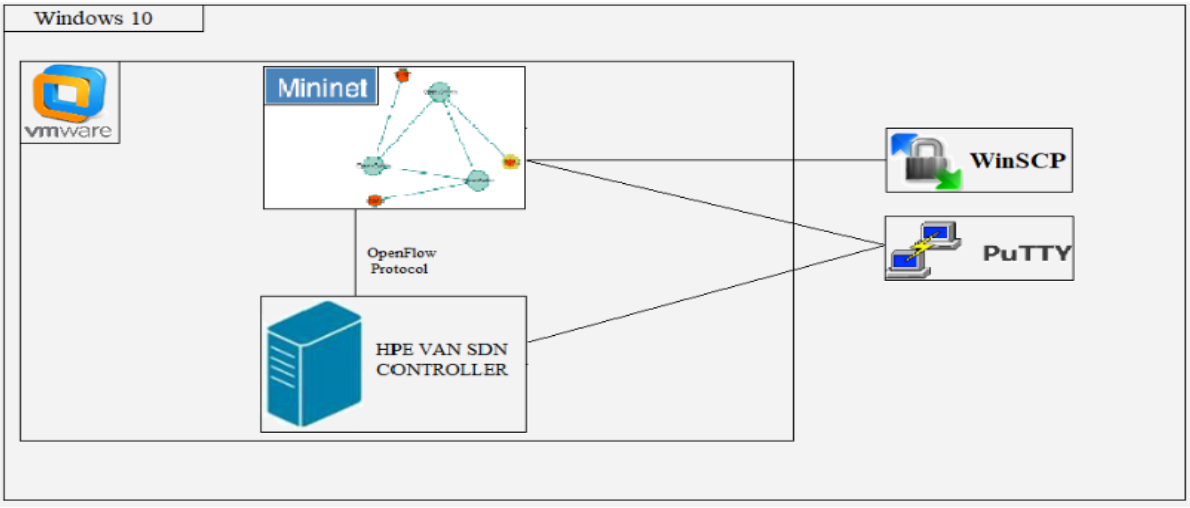


Рис. 1 Стенд для дослідження роботи віртуальної *SDN* мережі

Для конфігурування HPE VAN SDN controller використовуються програмні модулі написані на мові Python, тому саме Python був обраний для інтеграції власноруч написаного програмного модулю. А саме були, розроблені скріпти для дослідження кастомних (не типових) топологій. В подальшому, планується створення правил для оптимізації розподілу трафіку за допомогою мови програмування *Python* та розміщення їх на HPE VAN SDN controller.

Нестеров О.М. (НУОУ)
Зінченко І.А. (ВІТІ)
Зінченко М.О. (ВІТІ)

МЕТОД ОЦІНКИ ПРОПУСКНОЇ СПРОМОЖНОСТІ СИСТЕМИ ЗВ'ЯЗКУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ НА ОСНОВІ ДЕНДРОГРАМИ З ТИПОВИМИ МОДУЛЯМИ ЗВ'ЯЗКУ

Актуальність. При плануванні та експлуатації системи зв'язку спеціального призначення (СЗСП) виникає проблема у визначені її потрібної пропускної спроможності. Існуюча методика ґрунтується на простому арифметичному сумуванні потоків даних від різних джерел з врахуванням емпіричного коефіцієнта вибухоподібності трафіку, який необхідний для врахування збільшення пікового навантаження у СЗСП під час активізації роботи органів управління. Результатами її практичного застосування є надмірне значення показника пропускної спроможності СЗСП, що призводить до завищення на етапах створення та експлуатації її вартості.

Існує інший підхід для оцінки пропускної спроможності СЗСП, як основного показника під час планування її розгортання. Він спирається на відомі теорії масового обслуговування і телетрафіка. Відповідно цим теоріям, задача планування СЗСП поділяється на два етапи. Спочатку визначається необхідна пропускна спроможність вузлів зв'язку спеціального призначення (ВЗСП) пунктів управління (ПУ) та ліній прямого зв'язку, що їх з'єднують. Потім ці результати пов'язуються між собою за допомогою використання різного роду моделей і спрощень стосовно існуючих інформаційних напрямків у системі зв'язку.

Мета. Розробити метод обчислення пропускної спроможності СЗСП за окремими елементами та у цілому для оптимізації процесу її планування.

Основні положення. Метод ґрунтується на припущені щодо симетричності модуля зв'язку, тобто однаковій абонентської ємності і параметрах абонентського навантаження всіх ВЗСП, що входять до модуля зв'язку. Такий підхід враховує типові організаційні структури та модульний принцип побудови СЗСП. Для несиметричних модулів зв'язку запропоновано спосіб приведення їх до симетричного вигляду за рахунок віртуальної декомпозиції нетипового обладнання ВЗСП модуля зв'язку до стандартного вигляду. Введені припущення дозволяють розділити СЗСП, що досліджується, за допомогою методів кластерного аналізу на множину об'єктів за однорідними властивостями або кластери (групи). Під кластеризацією розуміється об'єднання об'єктів з максимально схожими властивостями в одну групу. Схожість об'єктів визначається вибраною метрикою. У якості метрики будемо застосовувати тактико-технічні характеристики телекомунікаційного обладнання та рівень ієрархії в системі управління.

Скористаємося методом ієрархічної кластеризації та проведемо її "знизу до гори". Використання запропонованого методичного прийому можливе і при використані іншого нетипового телекомунікаційного обладнання, здійснюючи нормування абонентського навантаження за абонентським навантаженням еталонного ВЗСП. Таким чином отримаємо кількість умовних ВЗСП, за прикладам перерахунку пропускної спроможності в умовні канали зв'язку. Синтезований метод дозволив провести удосконалення існуючої методики визначення необхідної пропускної спроможності системи СЗСП з ієрархічною топологією за рахунок переходу від арифметичного сумуванні потоків даних різних джерел до сумування ефективної швидкості передавання інформації від модулів зв'язку у відповідності з дендрограмою СЗСП. Впровадження одержаних наукових результатів у діяльність органів управління зв'язком дозволить провести економію ресурсів СЗСП на етапах її проектування та експлуатації. Напрямком подальших досліджень можливо вважати узагальнення запропонованого підходу на випадок більш складної топології СЗСП, визначення її оптимальної структури і провести оптимальний розподіл ресурсу пропускної спроможності телекомунікаційної транспортної мережі СЗСП між модулями зв'язку.

к.т.н. Овсянніков В.В. (НЦЗІ ВІТІ)
Гаврилюк О.Г. (НЦЗІ ВІТІ)
Черниш Ю.О. (НЦЗІ ВІТІ)

РЕАЛІЗАЦІЯ ПОСЛУГИ “ІДЕНТИФІКАЦІЯ І АВТЕНТИФІКАЦІЯ ПРИ ОБМІНІ” В МІЖНАРОДНИХ СТАНДАРТАХ

Постановка завдання. При побудові КСЗІ розподілених ІТС однієюз важливих послуг безпеки є послуга “Ідентифікація і автентифікація при обміні”. Вимоги до даної послуги викладено у НДТЗІ2.5-004-99. При впровадженні концепції НАТО FMN(FederatedMissionNetworking) виникає необхідність використання при оцінки захищеності ІТСміжнародного стандарту ISO-15408.

Мета роботи.Встановлення відповідності меж вимогами НД ТЗІ та вимогами стандарту ISO-15408 за цією послугою.

Результат дослідження. Відповідно до НДТЗІ 2.5-004-99послуга „Ідентифікація і автентифікація при обміні” дозволяє одному комплексу засобів захисту ідентифікувати інший комплекс засобів захисту (встановити і перевірити його ідентичність) і забезпечити іншому комплексу засобів захисту можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації. Ця послуга обов’язкова в розподілених ІТС (АС класу 3).

В стандарті ISO-15408 прийнятий інший підхід до оцінки захищеності. Стандартом визначено 11 класів, які детально розглядає вимоги до різних аспектів до захисту інформації. Тому за кожну послугу безпеки, яка вказана в НДТЗІ 2.5-004-99 відповідає кілька вимог з різних класів стандарту ISO-15408 Порядок зіставлення функціональних компонентів безпеки, визначених ISO-15408 з вимогами НД ТЗІ 2.5-004-99 визначені в НД ТЗІ 2.6-002-2015. Однак, в окремих випадках можливе неоднозначне тлумачення вимог нормативного документа, що приведе до помилок при оцінці захищеності.

НД ТЗІ 2.6-002-2015 дозволяють правильно визначитивимоги до послуги „Ідентифікація і Автентифікація при обміні” рівня НВ-1 „Автентифіікація вузла” та НВ-2 Автентифікація джерела даних”. В той же час помилкове визначення вимог можливо для рівня НВ-3 „Автентифікація з підтвердженням”.

Послуга НВ-3 визначає, що використовується протокол автентифікації повинен забезпечувати можливість однозначного підтвердження джерела об’єкта незалежною третьою стороною. Така можливість необхідна в ІТС об’єктів критичної інфраструктури та ІТС військового призначення.У сучасних системах автентифікація як користувачів так і комплексів засобів виконується виключно з використанням криптографічних алгоритмів та криптографічних протоколів. Стандарт ISO-15408вимагає вказати які алгоритми та протоколи використаються для цілейавтентифікації, однак не накладає обмежень наалгоритми та протоколи яки можуть використовуватися. В кожному випадку власник системи самостійно може визначати необхідні протоколи та алгоритми або стандарти автентифікації. Механізмиавтентифікації, які можуть бути використані в захищених системахвизначені у міжнародному стандарті ISO/IEC 9798 В цьому стандарті визначено 5 механізмів автентифікації. Із них тільки механізм заснований на цифровому підпису дозволяєзабезпечувати можливість однозначного підтвердження джерела об’єкта незалежною третьою стороною. Тому при реалізації послуги НВ-3 в ІТС об’єктів критичної інфраструктури та в системах військового призначення додатково к вимогам ISO-15408 обов’язково необхідно вказуватися вимоги щодо використання для цілій автентифікаціїISO/IEC 9798*Part 3: Mechanismsusingdigitalsignaturetechniques* .

Висновки. На підставі зіставлення вимог міжнародних стандартів та нормативних документів системи ТЗІ визначено додаткова вимога до ІТС об’єктів критичної інфраструктури та систем військового призначення,в яких повинно бути реалізована послуга НВ-3 “Автентифікація з підтвердженням”.

Овсянніков В.В. (ВІТІ)
Паламарчук Н.А. (ВІТІ)
Паламарчук С.А. (ВІТІ)
Чередниченко О. Ю. (ВІТІ)

ПІДХОДИ ДО ФОРМУВАННЯ ВИМОГ ІЗ ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ПІД ЧАС РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ АВТОМАТИЗОВАНИХ СИСТЕМ

У Збройних силах України розробляються та впроваджуються різноманітні проекти інформатизації, які спрямовані на підвищення ефективності та поліпшення якості управління процесами повсякденної та бойової діяльності військ [1]. Життєвий цикл кожної інформаційної (автоматизованої) системи розпочинається із задуму про її створення, далі вона проходить етапи проектування, випробовувань та впровадження. Для інформаційних систем (АС) передбачено вісім стадій її створення та експлуатації: формування вимог до АС; розроблення концепції системи; розроблення технічного завдання на створення; ескізне та технічне проектування; виготовлення робочої документації; введення в експлуатацію АС; супроводження АС [2].

Захист інформації в автоматизованих системах є складовою частиною робіт з їх створення та експлуатації, і повинен здійснюватися *на всіх етапах життєвого циклу АС*, на всіх технологічних етапах обробки інформації і в усіх режимах функціонування. Захищені АС не розглядаються окремо від інформації, яка в них обробляється. Інформація, яка належить до державних інформаційних ресурсів або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в АС із застосуванням комплексної системи захисту інформації (КСЗІ) з підтвердженою відповідністю [3].

КСЗІ системи являють собою сукупність організаційних заходів та технічних засобів, спрямованих на забезпечення захисту інформації, яка обробляється, зберігається та передається в АС, від загроз несанкціонованого доступу до неї [4, 5].

Згідно статті 8 [3] для створення КСЗІ, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації.

Діюча нормативно-правова база України щодо проектування та створення КСЗІ, дозволяє одночасно створювати АС та КСЗІ. Однак, доволі часто роботи зі створення АС виконуються окремо від створення КСЗІ, без узгодження організаційно-технічних рішень. Крім цього, досить часто виконання функціональних задач доцільно реалізувати на тій чи іншій архітектурі АС та/або за допомогою окремого програмного забезпечення (ПЗ), яке згідно [6] може бути загальним, функціональним та спеціальним (спеціальне програмне забезпечення розробляється під час створення АС).

Не рідко Замовники та Розробники ПЗ не висувають (не враховують) вимоги до захисту інформації, в частині розмежування доступу (так звані засоби захисту інформації, які реалізовані в обчислювальній системі АС) та не повністю усвідомлюють механізм впровадження розробленого ПЗ, особливо з врахуванням нормативних аспектів із захисту інформації.

На даний час в Збройних силах України спостерігається тенденція, коли ПЗ розробляється в ході створення АС (тобто, мова йде про спеціальне програмне забезпечення) або коли розробляється програмний комплекс, який планується встановлювати в уже діючі АС, в яких створена КСЗІ з підтвердженою відповідністю (програмний комплекс виконуватиме роль функціонального ПЗ). В подальшому, якщо в АС обробляється інформація з обмеженим доступом, буде проблематично встановити зазначене функціональне ПЗ на діючі об’єкти електронно-обчислювальної техніки, оскільки це ПЗ не

проходило експертизу в галузі технічного захисту інформації та не має відповідного експертного висновку.

Замовнику ПЗ доцільно було б, вимоги до захисту інформації визначати в ході його розробки (не залежно від того спеціальне чи функціональне), а їх деталізацію здійснювати на рівні окремо розробленого технічного завдання на створення ПЗ, що дозволить суттєво спростити механізм впровадження ПЗ в АС. Тобто, йти шляхом розробки ПЗ у відповідності з вимогами як до засобу технічного захисту інформації від несанкціонованого доступу, які визначені згідно [7].

За результатами аналізу вимог нормативних документів із захисту інформації та вимог, які висувалися Замовником до ПК "***", а також з врахуванням Критеріїв оцінки захищеності [8] можливо запропонувати наступний варіант функціонального профілю захищеності для ПК (АС надається для порівняння):

Варіант функціонального профілю захищеності для ПК "*"**	**Варіант функціонального профілю захищеності для АС**
{КА-2, КО-1, ЦА-1, ЦО-1, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НА-2},	{*КА-2*, КВ-1, *КО-1*, *ЦА-1*, ЦВ-1, *ЦО-1*, ДР-1, ДС-1, ДЗ-1, ДВ-1, *НР-2*, *НИ-3*, *НК-1*, *НО-2*, *НЦ-2*, НТ-2, НВ-1, *НА-2*},

Звідси, послуги безпеки, що стосуються конфіденційності та цілісності при обміні в АС та автентифікації вузла (КВ-1, ЦВ-1 та НВ-1), реалізуються за допомогою шифратора (засобу криптографічного захисту інформації), інші послуги безпеки (*10 із 18*) можливо реалізувати за рахунок програмного забезпечення, яке розробляється.

Висновки. За результатами аналізу вимог нормативних документів із захисту інформації та практичного досвіду запропоновано вимоги із захисту інформації від несанкціонованого доступу, які можуть бути реалізовані за допомогою ПЗ. Зазначене дозволить спростити організаційно-технічні рішення на створення АС, знизити її вартість (не використовуючи додаткових комплексів засобів захисту від несанкціонованого доступу, типу „Лоза", „Рубіж", „Гриф" тощо), зберегти обчислювальний ресурс АС та спростити роботу користувача в АС.

ЛІТЕРАТУРА

1. Галаган В.І., Бондарчук С.В. Полішко С.В. Застосування систем підтримки прийняття рішень в управлінні нерухомим військовим майном Збройних сил України – К : ЗНП ЦВСД НУОУ, випуск № 2 (63), 2018.

2. ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы стадии создания.

3. Закон України „Про захист інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" // Відомості Верховної Ради України. – 1994. – № 31.

4. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.2006 № 373 // Офіційний вісник України. – 2006. – № 13.

5. „НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу".

6. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.

7. „НД ТЗІ 3.6-001-00. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу" (зі змінами).

8. „НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу".

Оксьоненко М.П. (НТУУ „КПІ”)
к.т.н. Яковлєв С.В. (ВІТІ)

МЕТОДИ ВИЯВЛЕННЯ ПРИХОВАНИХ ФЕЙСТЕЛЬ-ПОДІБНИХ ПЕРЕТВОРЕНЬ

Актуальність. Одним із найпоширеніших методів криптографічного захисту конфіденційності інформації є симетричні блочні шифри. Питання їх стійкості завжди є актуальним через широке використання у різних системах захисту інформації. Одним із найпоширеніших методів побудови блочних шифрів є мережі Фейстеля. Мережі Фейстеля набули популярності через те, що вони можуть бути ефективно реалізовані (як апаратно, так і програмно) й мають досліджені криптографічні властивості. В зв'язку з такою популярністю з’явились деякі різновиди мереж Фейстеля (*MISTY*, *R*-схема), які можуть відрізнятися складністю реалізації та алгебраїчними властивостями. Наявність у криптографічному перетворенні внутрішньої структури фейстель-подібного перетворення дозволяє більш ефективно його реалізовувати та може закладати певні небажані алгебраїчні властивості. Через це набули розвитку методи, які дозволяють розпізнавати у таблично заданих перетворення приховані алгебраїчні структури типу схеми Фейстеля.

Мета. Метою роботи є розвиток та уточнення методів виявлення прихованих аналітичних структур на основі обчислення індикаторних матриць високого порядку.

Основна частина. Виявлення прихованих фейстель-подібних структур проводиться на основі вигляду індикаторної матриці високого порядку (*High-Degree Indicator matrix, HDIM*). Для *n*-бітової перестановки *F* індикаторна матриця високого порядку має вигляд:

$$\tilde{H}(F)[i,j] = \sum_{x \in F_2^n} (e_i \cdot F(x))(e_j \cdot x) \bmod 2$$

Коефіцієнти матриці $\tilde{H}(F)$ показують присутність найвищого степеня в координатних функціях F. Максимальна степінь d схеми Фейстеля й кількість раундів r корелюють з наявністю прихованих структур функції $\theta(d,r) = d^{\lfloor r/2 \rfloor - 1} + d^{\lceil r/2 \rceil - 1}$.

В роботі доведені теореми, які показують, як поводить себе HDIM на різних модифікаціях схеми Фейстеля, зокрема, для схеми MISTY. Нехай F – $2n$-бітна схема MISTY з *r* раундами та раундовим перетворенням *f*, $\deg(f_i) \le d$, $\deg(f_i^{-1}) \le D$. Елемент $\tilde{H}(F)[i,j]$ дорівнює нулю тоді та тільки тоді, коли виконуються наступні умови.

1. Для $i < n$:
   a. $r = 4l + 3$ та $\theta = d^{l+1} + D^{2l+1} < 2n$
   b. $r = 4l + 2$ та $\theta = d^{l+1} + D^{2l} < 2n$
   c. $r = 4l + 1$ та $\theta = d^{l} + D^{2l} < 2n$
   d. $r = 4l$ та $\theta = d^{l} + D^{2l-1} < 2n$
2. Для $n \le i < 2n$:
   a. $r = 4l + 3$ та $\theta = d^{l} + D^{2l+1} < 2n$
   b. $r = 4l + 2$ та $\theta = d^{l} + D^{2l} < 2n$
   c. $r = 4l + 1$ та $\theta = d^{l} + D^{2l} < 2n$
   d. $r = 4l$ та $\theta = d^{l} + D^{2l-1} < 2n$

Наведені співвідношення дозволяють виявляти приховані MISTY-схеми у таблично заданих перетвореннях, якщо зберігається певний баланс між кількістю раундів та степенем раундового перетворення. **Висновок**. Були сформовані й доведені теореми, які дозволяють виявляти внутрішню фейстель-подібну структуру перетворень з невідомим аналітичним описом. Розпізнавання таких структур базується на обчисленні індикаторної матриці високого порядку, яка залежить від кількості раундів та степені раундової функції. Сформульовані критерії, на основі яких можна висувати припущення про внутрішню структуру перетворень, а саме, про наявність прихованих фейстель-подібних схем.

Ольшанський В.В. (ВІТІ)
Кухар І.Г. (ВІТІ)
Єгоров Ю.А. (А0565)

АВТОМАТИЗОВАНА СИСТЕМА УПРАВЛІННЯ „КРОПИВА”

Автоматизована система управління вогнем артилерії „Кропива” – це програмно-апаратний комплекс, який об’єднує в собі засоби розвідки, управління і вогневого ураження в єдину інформаційну систему. Однією з найважливіших функцій цієї системи є корегування та підвищення точності вогню всіх видів артилерії. У військах зараз використовується кілька тисяч планшетів зі встановленою програмою „Кропива”. Тому під час виконання завдань за призначенням військовослужбовці ЗСУ можуть подавати запит на використання вогню артилерії зі звичайного планшета. Разом з тим, ця система постійно покращується, що робить систему більш досконалою і зручною у використанні.

Головною метою ПАК „Кропива” є підвищення ефективності ураження цілей шляхом поєднання апаратних і програмних засобів, картографічного забезпечення, автоматизації розрахунків, а також передачі команд та цілевказань через цифрові канали зв’язку.

Систему можна під’єднати до будь-якого планшета, якщо встановити спеціальну прошивку. Для керування та передачі команд „Кропива” використовує короткохвильові та ультракороткохвильові цифрові радіостанції, що відповідають стандартам захищеного зв’язку військ НАТО. Однією з головних переваг використання ПАК „Кропива” є скорочення часу розгортання вогневої батареї (скорочується майже в п’ять разів), та часу, що потрібний для підготовки до бойового застосування – скорочується втричі.

В програмі передбачена функція, що дозволяє знімати данні про погоду не тільки загального прогнозу, але і з портативних метеостанцій, розташованих прямо на позиціях і навіть з приладів, що входять до складу окремих снайперських комплексів.

Для підвищення ефективності системи „Кропива” було покладено максимум зусиль та мінімум часу для як найкращого управління артилерійським вогнем з допомогою програмного забезпечення, яке „прошивається” на будь-який пристрій, який підтримує систему Android. Цим самим було спрощено використання в бойових умовах корегування артилерійського вогню з допомогою простих доступних гаджетів.

Ще на початку бойових дій в 2014 році воєнні відчували гостру нестачу систем управління вогнем та засобів контрбатарейної боротьби. Артилеристам доводилося здійснювати розрахунки для наведення гармат за допомогою спеціальних таблиць або навіть в розумі. Виходом з цієї ситуації було встановлення на планшет offline-карти зони бойових дій, щоб допомогти військовим краще орієнтуватися на місцевості.

З огляду на широке поширення „Кропиви” у військах і велику кількість інформації про розташування вогневих точок противника, працювати з комплексом цієї системи дуже просто. Для цього потрібно знати координати цілі і місця розташування своєї артилерійської батареї. Ці данні вводяться в планшет, який обчислює точний напрям стрільби і відстань до цілі. В системі „Кропива” заздалегідь закладені докладні тактико-технічні данні всіх типів артилерійських систем і боєприпасів, що є на озброєнні ЗС України. Комплекс також допомагає стріляти з танків зі стаціонарних позицій. Далі вводиться в планшет характеристики зброї і боєприпасів, враховуються метеоумови (швидкість і напрям вітру, температуру повітря, вологість і т. д.) і таким чином розраховуються найточніші параметри удару. Швидкість обчислення обмежується тільки швидкістю набору тексту.

Систему „Кропива” може підтримувати будь-який пристрій, що має платформу Android. Розміщене програмне забезпечення забезпечує перевагу в часі та точності ведення вогню з урахуванням умов обстановки та використання вогневих засобів. Дружній та зрозумілий інтерфейс дозволяє будь-якому мало навченому військовослужбовцю досить легко навчитися та виконати поставлене завдання щодо коректування та нанесення артилерійського вогню по позиціях противника.

Остапук О.І. (ВІТІ)
Гришина Н.С. (ВІТІ)
Карабань О.В. (ВІТІ)
Побережець Т.В. (ВІТІ)

ВАРІАНТИ ВИРІШЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В МУЛЬТИСЕРВІСНІЙ МЕРЕЖІ ЗВ'ЯЗКУ

Традиційні методи захисту телекомунікаційних мереж орієнтовані на захист від конкретних (відомих або прогнозованих) видів загроз атак. Вони реалізуються у вигляді набору програмних та апаратних компонентів, функціонуючих відносно незалежно один від одного, а існуючі системи захисту зазвичай мають централізовану структуру, характеризуються не розвиненими адаптаційними можливостями, пасивними механізмами виявлення атак, великим відсотком помилкових спрацьовувань при виявлені вторгнень, значною деградацією трафіка цільових інформаційних потоків через великий об'єм ресурсів, що виділяються на захист і т.п.

Тому в останні роки рішення цих задач покладається на автоматизовано керовані комплекси технічних засобів, які дозволяють суттєво (порівняно з традиційними) підвищити ефективність захисту інформації, в тому числі її адекватність, відмовостійкість, стійкість до деструктивних дій, універсальність, гнучкість і т.п.

Припускається, що компоненти перспективних систем захисту інформації в мультисервісній мережі зв'язку, діють за єдиним планом, тісно взаємодіють один з одним з метою обміну інформацією та прийняття узгоджених рішень, адаптуються до змін трафіка, реконфігурації апаратного та програмного забезпечення, а також новим різновидам атак.

Функціонування мультисервісних мереж з високим показником по ефективності в умовах інформаційної протидії та досить жорстких вимог до них з боку різних користувачів (посадових осіб органів управління), можливе тільки при вирішенні цілого комплексу завдань забезпечення інформаційної безпеки. Вирішальну роль у ньому відводиться автоматизованій системі управління мережею.

Значна складність мереж, що входить до складу мультисервісних мереж зв'язку (абонентські мережі, мережі доступу, транспортні мережі, мережі надання послуг прикладного рівня), та механізми захисту інформації, які в них реалізуються, збільшують кількість вразливостей пов'язаних із застосуванням стандартних протоколів, наявність потенційних помилок або „закладок" у програмному забезпеченні засобів телекомунікацій, засобів надання послуг зв'язку та управління, а також високій ймовірності уражень при реалізації різного роду атак, обумовлюють необхідність розробки досить складних автоматизованих комплексів управління мережевою безпекою, до складу яких входять потужні адаптовані засоби виявлення та аналізу цих атак.

Такі комплекси здатні не тільки контролювати працездатність засобів захисту інформації в кожній мережі, а й суттєво підвищити захищеність елементів мультисервісної мережі зв'язку від інформаційного впливу, існуючих помилок в конфігурації кожної мережі, сприяти виявленню можливих трас атакуючих дій різних категорій порушників (при реалізації ними різних загроз безпеки), визначити критичність мережевих ресурсів, а також здатні підготувати данні щодо корегування чи вибору нової політики безпеки, адекватній існуючій загрозі.

При вирішенні задачі забезпечення інформаційної безпеки пропонується використовувати наступні моделі: мультисервісні мережі зв'язку, атаки порушника, а також графа атак**.**

Модель мультисервісної мережі зв'язку (ММЗ).

ММЗ слугує для уявлення в системі управління даної мережі програмного та апаратного забезпечення, розпізнання дій противника та визначення реакції мережі на його атакуючі дії. При цьому в модель мережі доцільно вбудувати модель розпізнання дій

порушника, яка дозволить здійснити перетворення низькорівневого представлення атакуючих дій (послідовність „хибних” мережевих пакетів або «хибних» команд для операційної системи) у високорівневі ідентифікатори атак.

Модель атак**.**

Модель програмно – апаратних атак використовується для описання можливих дій противника і як правило, модель має вид ієрархічної структури, що складається з декількох рівнів (комплексний, сценарний).

Модель противника тісно пов’язана з моделлю атак. Взаємозв'язок цих двох моделей полягає в тому, що в моделі атак знаходиться максимально повний опис можливих способів компрометації об’єктів мультисервісної мережі зв’язку, а модель противника конкретизує хто і якими засобами може реалізувати дані загрози та завдати шкоду тому чи іншому об’єкту мережі. При цьому сама модель повинна враховувати основні параметри противника:

початкове положення внутрішній чи зовнішній противник;

рівень знань, вмінь противника по реалізації атакуючих дій (задається переліком відомих противнику слабих місць, засобів реалізації атак і т.п.);

початкові відомості про мультисервісну мережу зв’язку, що атакується (у вигляді переліку термінальних пристроїв, комутаторів, маршрутизаторів, серверів, користувачів і т.п.);

метод, який використовується генерацією сценарію.

Модель графа атак.

Для більш детальних сценаріїв різних атак часто застосовують модель формування загального графа атак, який служить для побудови графа, що буде описувати різні варіанти реалізації атакуючих дій описання противника з врахуванням його початкового положення, рівня знань та навичок, конфігурації мультисервісної мережі зв’язку та політики безпеки, що в ній реалізується.

На основі побудованого графа атак, проводиться аналіз захищеності ММЗ, а також визначають «вузькі» місця мережі, на основі чого виробляють рекомендації по усуненню виявлених уражень із врахуванням їх рівня критичності.

Об’єкти графа атак діляться на базові об’єкти та складові, причому вершини графа задаються з використанням базових об’єктів, а для формування різних послідовностей дій порушника базові об’єкти зв’язуються на графі атак за допомогою дуг. Таким чином, формуються складові об’єкта графа. До базових об’єктів загального графа атак на мультисервісну мережу зв’язку відносяться об’єкти, які належать багатьом «атакуючим діям» складаються з усіх елементарних дій порушника.

Атакуючі дії розділили на:

дії на отримання інформації про мультисервісну мережу зв’язку та її елементи, тобто розвідувальні дії;

дії, які готуються (в рамках вже існуючих у порушника повноважень), які слугують для створення умов реалізації атакуючих дій наступних класів;

дії, які направлені на порушення конфіденційності;

дії, з порушення цілісності;

дії, які направлені на порушення доступності;

дії, які призводять до отримання противником прав локального користувача;

дії, які призводять до отримання прав адміністратора.

До складових об’єктів графа атак відносяться об’єкти типів «траса», «загроза», та «граф», при цьому під трасою атаки розуміється сукупність зв’язаних вершин загального графа атак (АРМ, серверів, комутаторів, маршрутизаторів та атакуючих дій), перший елемент траси – відповідає начальному положенню порушника, а останній не має вихідних дуг. Під загрозою розуміється багато різних трас атак, які мають однакові початкову та кінцеву вершини.

Поділ атакуючих дій відповідає класифікації загроз у відповідності з відомими типами:

загальні загрози – загрози порушення конфіденційності, цілісності, доступності;

додаткові загрози – загрози отримання інформації про мультисервісну мережу зв'язку (АРМ, сервери, комутатори, маршрутизатори), загрози отримання порушником прав локального користувача або прав адміністратора.

Однак при успішній реалізації порушником розвідувальних дій в мультисервісній мережі зв'язку не відбувається порушення ні конфіденційності, ні цілісності, ні доступності інформаційних ресурсів мережі.

При успішному отриманні порушником прав локального користувача, можливості виконання дій, спрямованих на порушення конфіденційності, цілісності та доступності, або на отримання прав адміністратора збільшення, але відбувається це тільки тоді, коли він сам зробить відповідні дії.

При успішному отриманні прав адміністратора на певному АРМ або сервері порушник здатен повністю порушити конфіденційність, цілісність, доступність всіх об'єктів даного вузла мультисервісної мережі зв'язку або навіть фрагменту мережі.

В напрямку росту ступеня складності всіх об'єктів графа атак упорядковуються таким чином: елементи мережі → атакуючі дії → траси атак → загрози → загальний граф атак.

Після реалізації кожного сценарію, який належить безлічі сценаріям розвідки, здійснюється перевірка умов виконання атакуючих дій, враховуючи вразливості програмного та апаратного забезпечення елементів мультисервісної мережі зв'язку. При успішній реалізації атакуючих дій заданої групи, яка призводять до отримання противником прав локального користувача або адміністратора на атакованому АРМі або сервері, відбувається перевірка необхідності переходу на даний елемент мережі. У випадку реалізації переходу, ця послідовність дій повторюється для нового положення противника.

Для оцінки рівня захищеності мультисервісної мережі зв'язку можна застосувати спрощений експрес метод інтелектуальної системи аналізу, який складається з наступних етапів:

визначення рівня критичності елементів мультисервісної мережі зв'язку по спрощенню трирівневої шкали (високий, середній, низький);

визначення критичності атакуючих дій;

визначення розміру збитку, викликаного успішною реалізацією атакуючих дій, залежного від рівня критичності дій та атакуючого елемента мережі;

визначення розміру збитку для всіх загроз;

визначення метрик складності доступу для всіх атакуючих дій у всіх трасах, з врахуванням даного показника для кожного з дій, складаючи трасу, і всіх загроз, з врахуванням значень даного показника для всіх трас, складаючи загрозу.

Загальним видом потоку впливу є рекурентний потік, характеризується він тим, що інтервали часу між двома інформаційними впливами незалежні та мають однакові довільні функції розподілу $F(t)$, а також потік Бернуллі, який характеризується тим, що дає можливість одночасно надходити одразу декільком впливам, кількість джерел впливу обмежена, а кожне джерело за визначений інтервал часу може генерувати тільки один вплив, (потік, в якому інформаційний вплив надходить незалежно та їх число в інтервалі часу фіксовано).

Таким чином, використовуючи модель мультисервісної мережі зв'язку, модель атаки порушника, графа атак при вирішенні задачі забезпечення інформаційної безпеки в контурі управління мережевої безпеки підсистеми управління мережею, з'являється можливість ефективно та детальніше протидіяти передбачуваним загрозам, які в теперішній час існують в арсеналі потенційного противника. Це в свою чергу дає можливість прогнозувати наслідки таких загроз та завчасно приймати організаційні, технічні та інші заходи по їх мінімізації.

к.т.н. Орлов В.В. (ВА м. Одеса)
Симоненков В.М. (ВА м. Одеса)

РОЗВИТОК ПАСИВНИХ СИСТЕМ ЗВУКОВОЇ ЛОКАЦІЇ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ В УМОВАХ ТЕРОРИСТИЧНИХ ЗАГРОЗ

Стрімкий розвиток інформаційно-управляючих систем і засобів автоматизації керування безпілотним літальними апаратами (БпЛА) створює загрози для об'єктів критичної інфраструктури ЗС України. Несвоєчасне виявлення терористичних загроз із використанням БпЛА, наприклад, у Сирії й Саудівської Аравії, спричинило значні людські втрати та катастрофічні збитки нафтових компаній.

Для підвищення достовірності у системах підтримки прийняття рішень виявлення терористичних загроз, як правило, застосовується комплексування інформаційних технічних систем, що засновані на різноманітних фізичних принципах: від радіолокації, сейсмолокації, контролю й управління доступом до телевізійного спостереження, тепловізорів та оптичних систем тощо.

На жаль, має місце низька ефективність виявлення малорозмірних БпЛА, які внаслідок малої поверхні, що відбиває, та низької висоти польоту – невидимі для РЛС і засобів радіоелектронної боротьби. Крім того, існуючи відеозасоби моніторингу також малоефективні через апріорну невизначеність щодо напрямку й часу „атаки” БпЛА-порушника.

Одним з перспективних напрямків спостереження є застосування систем, які захищені від засобів радіоелектронної боротьби, зокрема, пасивних систем звуколокації, але, на цей час, не вирішене завдання визначення координат БпЛА, як джерела звукових сигналів, що рухаються в тривимірному просторі.

У якості базової системи було розглянуто звукометрічний комплекс артилерійської розвідки АЗК-7, який був розроблений на підприємстві СКБ „Молнія” (м.Одеса) та перебував на озброєнні колишнього СРСР. Сигнали з виходів просторово-рознесених датчиків близькі за формою, але розрізняються за часом, зашумлені (перетворені) за рахунок вітру та середовища поширення.

Під час досліджень були розглянуті та проаналізовані записи акустичних сигналів, визначені спектральні характеристики низки БпЛА, дронов і літаків, які показали принципові можливості побудови систем ЦОС і виявили особливості конкретних літальних апаратів для їхнього розпізнавання. За допомогою отриманих в результаті фізичних експериментів даних, в середовищі Matlab було створено програму імітаційного моделювання системи моніторингу, виявлення й визначення координат цілей (БпЛА), яка призначена для вибору конфігурації системи залежно від вимог до розміру зони контролю й точності визначення координат.

Отже, для контрольованої зони до 500 м помилка визначення координат БпЛА, що рухається, складає – 10 м. Помилки координат нерухомих джерел імпульсних аудіосигналів приблизно в 2 рази менше.

Таким чином, проведений аналіз системи звуколокації виявив потенційні можливості визначення координат БпЛА та інших рухомих об’єктів у тривимірному просторі з достатньою точністю для подальшого супроводження цілей засобами візуального спостереження.

Подальший розвиток алгоритмів доцільно проводити в наступних напрямках:

1. Розпізнавання класу рухомого повітряного об’єкту на підставі відмінностей у параметрах аудіоспектрів: літак або мультікоптер, з електричним двигуном або двигуном внутрішнього згоряння тощо.

2. Розроблення алгоритмів для одночасного визначення множини цілей.

Павленко К. І. (ЖВІ)

ПЕРСПЕКТИВИ РОЗВИТКУ ІНЖЕНЕРНИХ БОЄПРИПАСІВ В УМОВАХ ВЕДЕННЯ ГІБРИДНИХ ВІЙН

Обладнання і утримання інженерних загороджень є однією з основних завдань інженерних військ. З цією частиною бойової діяльності інженерних військ усі до деякої міри знайомі. На сам перед, це установка мінних полів. Мінні поля грають дуже істотну роль у прикриті позицій військ від атак супротивника.

Досвід ведення бойових дій під час проведення антитерористичних операцій, операцій об'єднаних сил на сході України свідчить про те, що мінна небезпека може дуже значно впливати на дії супротивника. Міни не настільки багато наносять реальної шкоди супротивнику, скільки впливають на психіку особового складу. Досвід показує, що досить підриву на мінах двох-трьох танків, щоб цілком зірвати атаку танкової роти, це свідчить про те, що достатньо підриву на міні однієї машини на дорозі для того, щоб швидкість руху колони супротивника знизилась від 1 до 5 км/год. У бойових статутах ряду країн існує термін „мінна війна". Масове застосування мін здатне навряд чи не цілком паралізувати будь-яку бойову діяльність військ супротивника на тій чи іншій території.

У даний час мінна безпека підсилюються тим, що розвиток техніки й електроніки дозволяє створювати навряд чи нерозумні міни. Це реальність, що міна не реагує на солдата своєї армії, мирного жителя, але моментально спрацьовує при наближені до неї і вибухає у самий вигідний момент. Крім того, на сьогоднішній день немає ні єдиного досить надійного способу виявлення мін, і навіть при виявленні міни немає способів їхнього надійного знешкодження. Міни можуть мати датчики що розпізнають – ціль це, чи мінний трал, можуть розпізнавати значимість цілі, можуть мати прилад кратності (пропустити визначену кількість цілей і під наступною вибухнути). Міни можуть по радіосигналу переводитися в бойове чи безпечне положення, чи самоліквідуватися. Для установки мінних полів окремих мін зовсім не обов'язкова присутність сапера на місці установки. Міни можна ставити дистанційно (закидати навіть на територію супротивника за допомогою артилерії або авіації). Мінами можна в дуже короткий термін прикрити дуже великі ділянки фронту. Якщо на початку шістдесятих років саперний підрозділ за ніч міг встановити однин кілометр мінного поля, то зараз за годину до 10 – 15 кілометрів.

Науково-технічна думка у військовій сфері розвивається у багатьох напрямках. Одним із них є підвищення їх бойової ефективності інженерних боєприпасів. Так, значні технологічні перспективи розвитку мінно-вибухових пристроїв науковці вбачають у:

розробці новітніх зразків із застосуванням передових технологій у галузі штучного інтелекту та робототехніки;

застосуванні матеріалів, які матимуть здатність „маскуватися" під навколишнє середовище;

створенні активних датчиків цілі, які будуть мати здатність вести її пошук на відстані та розпізнавати за принципом „свій – чужий";

застосуванні у вибухових пристроях елементів, що будуть забезпечувати самодеактивацію (самоліквідацію) боєприпасів за визначених умов;

розробці зразків, здатних уражати об'єкти за умови відсутності безпосереднього впливу на датчик цілі та можуть керувати роботою 4–5 протипіхотних осколкових мін;

заміни чек підривників на датчики, які активуються (деактивуються) за допомогою електронного пристрою (ключа) з метою унеможливлення знешкодження їх противником тощо.

Таким чином, перспективними напрямками вдосконалення інженерних боєприпасів, є створення „розумних" і „підступних" пристроїв, які спроможні вибухати декілька разів підряд і які, надзвичайно важко знешкодити.

к.пед.н. Павленко О.А. (ВІТІ)

НАПРЯМКИ ЗАПРОВАДЖЕННЯ СИСТЕМ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ ПІД ЧАС ПІДГОТОВКИ ВІЙСЬКОВИХ ФАХІВЦІВ

Актуальність. Одним із перспективних напрямків підвищення рівня підготовки військових фахівців, на наш погляд, є використання систем імітаційного моделювання (далі – СІМ) в організації освітнього процесу у вищих військових навчальних закладах. У США та провідних країнах світу СІМ застосовуються у процесі підготовки військових фахівців з 1980-х років. За даними військових аналітиків, на сьогодні співвідношення реальних та змодельованих навчань становить близько 50:50, однак у майбутньому ситуація змінюватиметься у бік зростання частки віртуальних військових заходів з огляду на потреби країн в економії коштів на військові витрати та швидкий розвиток засобів штучного моделювання і відображення обстановки.

Мета. Дослідити можливості підготовки військових фахівців за допомогою імітаційного моделювання сучасного загальновійськового бою та тактики бойових дій у складі механізованих підрозділів на різній місцевості, включаючи райони населених пунктів.

Виклад основного матеріалу. Американські фахівці поділяють імітаційні моделі за призначенням на три основні групи:

– забезпечення аналізу та оцінки обстановки (оперативна робота);

– створення нових зразків озброєння та військової техніки;

– навчання особового складу, оперативної та бойової підготовки військ та штабів.

На теперішній час розрізняють наступні основні СІМ:

– реальні (live) системи, до яких відносяться традиційні військові і командно-штабні навчання (далі – КШН) із залученням штатної техніки та особового складу (бойові стрільби, проведення навчань у реальних умовах, проведення тренувань);

– віртуальні (virtual) системи представляють моделювання, в якому користувачі керують віртуальними системами (різні тренажери з керування озброєнням та військовою технікою, тренажери відпрацювання навичок прийняття рішень або навичок роботи у складі колективу);

– конструктивні (constructive) системи – процес роботи комп'ютерної програми, яка імітує дії особового складу, функціонування техніки та озброєння. Застосовуються для навчання тактиці дій у складі підрозділу під час бойових дій.

Переважаючою формою оперативної та бойової підготовки штабів з'єднань і частин сухопутних військ США є КШН (тренування) з відпрацюванням завдань розгортання частин і підрозділів як з використанням комп'ютерних систем моделювання бойових дій, так і в польових умовах. У перспективі очікується подальше глобальне комплексування моделей і впровадження систем віртуальної реальності (штучного багатовимірного бойового простору) на базі телекомунікаційних мереж, покликаних забезпечити доступ як до оперативного, так і фізичного модельованого середовища, стандартизованих моделей і баз даних, а також до різного роду сценаріїв.

На теперішній час американські компанії, які займаються розробкою програмного забезпечення засобів імітаційного моделювання, зосереджені над вдосконаленням розробки так званої 1st Person Shooter (стрілець від першої особи). Одним з перших серед кращих програмних забезпечень в цьому напрямі вважається VBS2 (далі – VBS2) – Virtual Battlespace 2 (Віртуальний бойовий простір). VBS2 – повністю інтерактивна тривимірна система підготовки, що забезпечує покращене штучне середовище, яке застосовується в різноманітних військових, навчальних та експериментальних цілях. Ця система надає змогу управляти бойовою технікою на суші, в повітрі та на морі. VBS2 може використовуватись для вивчення тактики дій та процедур під час наступальних, оборонних операцій, а також операцій патрулювання починаючи від окремого солдата до рівня відділення – взвод. У рамках запровадження модернізованої версії VBS3 важливою функцією стануть більш

реалістичні аватари, які дозволять військовослужбовцям розрізняти один одного за обличчям. Розробник BiSim планує запровадження режиму змішаної реальності, в якому військовослужбовці будуть „бачити фізичні об'єкти та взаємодіяти з ними".

Найбільшу кількість СІМ запроваджено в Національній академії сухопутних військ ім. гетьмана Петра Сагайдачного. Тут використовується три системи, які різняться між собою за рівнем підрозділу від відділення до бригади включно та складністю сценарію проведення тренувань, навчань.

Перша – Follow Me (надана компанією ALION Science and Technology) призначена для відпрацювання тактичних навичок ланки відділення – взвод. Follow Me InGEAR – це тактичний рівень, гра з прийняттям рішень, яка дозволяє курсантам проводити швидкі вправи на виконання, візуалізацію та планування, орієнтовані на планування, використовуючи імітаційне бойове середовище. Можливість розбору дій (AAR), вбудована у Follow Me InGEAR, дозволяє курсантам переглядати, аналізувати та вивчати кожну змодельовану операцію. Крім того, експерти надають курсантам під час гри поради; які будуть попереджати про потенційні небезпеки у ході поточних дій.

Друга – Battle Command (надана компанією ALION Science and Technology) для відпрацювання тактичних навичок рівня рота - батальйон. Програма Battle Command (Бойове Управління) - це засіб імітаційного моделювання, який дозволяє командирам підрозділів та офіцерам штабів відпрацьовувати заходи з планування та проведення бойових дій. Визначені плани дій відтворюються на змодельованому полі бою. Існує можливість проводити імітаційні дії в режимі одного чи декількох гравців, за необхідності приєднуватися до сценарію програм. Крім того, під час гри можна використовувати оверлеї, супровідну документацію, плани. Кожен сценарій прив'язаний до певної місцевості. У базі даних місцевості міститься тривимірна інформація про даний географічний район та навколишнє середовище, в якому будуть діяти підрозділи.

Останньою СІМ є JCATS (надана компанією CUBIC APPLICATIONS), що дозволяє проводити тренування, навчання до рівня об'єднання включно. На даний час запроваджена, крім Національної академії сухопутних військ, Національним університетом оборони України ім. Івана Черняховського. СІМ JCATS була створена Національною Лабораторією Лоренса Лівермора (США) та є однією з найпотужніших систем, представлених сьогодні на ринку конструктивних тренажерів.

СІМ JCATS надає можливості готувати війська до спектра властивих збройним силам завдань, моделювати тактику бойових дій в окремих групах та з'єднаннях на різній місцевості, включаючи райони міської забудови. СІМ JCATS призначена для моделювання дій підрозділів, частин, з'єднань та об'єднань згідно з прийнятим командиром рішенням у визначених умовах обстановки. Вона використовується для проведення КШН (тренувань) з метою набуття тими, хто навчається, практичного досвіду виконання службових обов'язків у реальних (бойових) умовах. Важливо, що всі дії моделюються на місцевості, а не на карті. Тому природні і штучні загородження впливають на здатність виявляти, стріляти і пересуватися. База даних місцевості включає лінії рельєфу, дороги, ріки, відкриті водоймища та рослинність, при цьому розміри карт можливо змінювати. СІМ JCATS дозволяє моделювати багатоповерхові будівлі із дверима, вікнами та стінами, а також підвальними приміщеннями, підземні ходи та тунелі.

Висновки. Застосування СІМ у підготовці військових фахівців в Україні дозволить:

– значно скоротити вартість тактичних, тактико-спеціальних та інших навчань, які проводяться в реальному вимірі на полігонах;

– урізноманітнити можливі сценарії бойових операцій, що дозволить досягти широкого спектру навчальних цілей та відпрацювати тактику і прийоми дій, які важко відтворити в реальному середовищі і вимагає певного допоміжного обладнання, несе ризики екологічній безпеці та життю і здоров'ю військовослужбовців;

– підвищити рівень тактичної підготовки командирів різної ланки, що в подальшому збереже життя та здоров'я військовослужбовців під час реальних бойових дій.

Пащетник В.І. (НАСВ)
к.т.н. Пащетник О.Д. (НАСВ)

МІЖДИСЦИПЛІНАРНА ІНТЕГРАЦІЯ ЗНАНЬ У ВИЩОМУ ВІЙСЬКОВОМУ НАВЧАЛЬНОМУ ЗАКЛАДІ

Сьогодення вимагає ефективного управління навчанням майбутніх офіцерів на науковій основі з урахуванням основних вимог до формування сучасного компетентного фахівця. Це, у свою чергу, передбачає пошук нових підходів до озброєння майбутніх фахівців міцними знаннями основ наук, формування в них свідомого ставлення до навчання, належного рівня професійної компетентності, а також суттєвого удосконалення змісту і методів навчання, підвищення ефективності навчально-виховного процесу в умовах вищого військового навчального закладу (ВВНЗ). Саме тому сьогодні проблематика міждисциплінарних зв'язків як системи, якою можна управляти як дидактичним засобом, що сприяє підвищенню ефективності професійної підготовки майбутнього фахівця, є актуальною і перспективною. Якість професійної підготовки майбутніх офіцерів значною мірою залежить від того, наскільки навчальні плани та структурно-логічні схеми забезпечують розкриття діалектичного взаємозв'язку між навчальними дисциплінами, а також здатності викладача викликати та постійно підтримувати у суб'єктів навчання інтерес до таких зв'язків. З огляду на це, найбільш раціонально використовувати міжпредметні зв'язки викладачеві задля підвищення ефективності мисленнєвої діяльності майбутніх фахівців. Дієвим шляхом вдосконалення процесу розвитку професійних компетенцій курсантів є комплексування дисциплін навчальних занять у ВВНЗ. Цикл навчальних дисциплін професійної підготовки включає в себе дисципліни загально-професійної, військово-професійної та військово-спеціальної підготовки.

Вивчення дисциплін всіх циклів повинно бути взаємопов'язане і проводитися в логічній послідовності, в тісному взаємозв'язку з тактикою, службово-бойовим застосуванням Сухопутних військ, об'єднуватися загальним задумом та побудовою, крім того забезпечувати отримання курсантами необхідних знань, умінь і навичок для успішних практичних дій на заняттях та при виконанні службово-бойових завдань.

Міждисциплінарна інтеграція знань на основі комплексування дисциплін як всередині одного, так і між різними циклами дозволяє:

– відображати актуальні міжнаукові зв'язки в змісті нормативної та варіативної частин професійної підготовки майбутніх офіцерів у ВВНЗ;

– обґрунтувати цілі, принципи, методи і засоби професійної підготовки майбутніх фахівців у ВВНЗ, за допомогою яких відбувається забезпечення міжпредметних зв'язків (МПЗ) у процесі викладання навчальних дисциплін спеціальної і фахової підготовки з фундаментальними дисциплінами;

– формувати і розвивати у курсантів основні компетенції при навчанні, сприяючи організації МПЗ і формуванню системного мислення сучасного фахівця;

– забезпечувати взаємну узгодженість навчальних програм із різних навчальних дисциплін і методик їх викладання з метою формування у курсантів комплексного наукового світогляду щодо конкретного виду фахової діяльності;

– сприяти формуванню діалектичного світогляду в процесі отримання загально-професійних, фахових і комунікативних знань, навичок, умінь ін.

Таким чином, інтеграція в педагогічній науці розуміється як процес і результат об'єднання компонентів змісту освіти, де, в свою чергу, МПЗ виступають інтегральним правилом у системі дидактичних принципів (науковості, системності, цілісності, професійної та особистісної спрямованості вищої військової освіти тощо), який визначає їх цільову спрямованість і сприяє формуванню у свідомості майбутніх офіцерів цілісної системи наукових знань про свою майбутню професійну діяльність у підрозділах Збройних Сил України.

к.т.н. Пащетник О.Д. (НАСВ)
к.т.н. Живчук В.Л. (НАСВ)
Поліщук Л.І. (НАСВ)

РОЗРОБКА ОНТОЛОГІЧНОЇ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ КОМАНДИРІВ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ СУХОПУТНИХ ВІЙСЬК ЗБРОЙНИХ СИЛ УКРАЇНИ

З метою розвитку автоматизованих систем управління військами та зброєю, їх програмно-математичного та інформаційного забезпечення постає необхідність щодо визначення раціонального складу та структури мережецентричної системи підтримки прийняття рішень (СППР) командирів тактичної ланки управління Сухопутних військ Збройних сил України.

Впорядкування та ефективне використання необхідної інформації для підготовки і ведення бойових дій командирами тактичної ланки управління можливе за умов побудови онтології предметної області впорядкованих та структурованих знань з використанням певної концептуалізації. Онтологія для СППР автоматизованої системи управління військами (АСУВ) будується на основі знань, формалізованих у бойових статутах і інших керівних документах із врахуванням стандартів НАТО щодо обміну інформацією, структури баз даних, а також програмної реалізації моделей, методів та алгоритмів функціонування окремих модулів СППР.

З цією метою та на підставі вимог Державної програми розвитку Збройних сил України на період до 2020 року (розділ „Стратегічні цілі") та Плану основних заходів щодо переходу Збройних сил України на стандарти НАТО, який затверджений Міністром Оборони України 19 жовтня 2015 року, у Науковому центрі Сухопутних військ Національної академії Сухопутних військ імені гетьмана Петра Сагайдачного проводиться ряд досліджень щодо створення системи підтримки прийняття рішень (СППР) командирів тактичної ланки Сухопутних військ за стандартами НАТО, зокрема FM 3.0 Operations, FM 5.0 The operations process, FM 6.0 Commander and Staff Organization and Operations та інші.

Для створення спеціального програмного забезпечення, яке реалізує функції СППР, розроблено ієрархічну структуру, верхнім рівнем якої є відомі сім етапів (кроків) процесу прийняття рішень MDMP (The Military Decision-Making Process). Наступним рівнем є підетапи, а далі – задачі, які виконуються на відповідних підетапах. В зазначеній ієрархічній побудові є складові елементи задач, а також підказки, які надаються відповідному командиру при їх виконанні. Такими підказками можуть бути: різні форми документів, які відпрацьовуються на відповідних етапах (підетапах); інформаційно-розрахункові задачі; тактичні приклади; посилання на керівні документи або їх розділи (глави, пункти), які регламентують виконання конкретних задач; посилання на довідники; каталоги.

Таким чином, формування мережецентричної онтологічної системи підтримки прийняття рішень на ведення бойових дій командирів тактичної ланки управління (батальйон, бригада і вище) із урахуванням стандартів країн-членів НАТО, надасть користувачам можливість роботи у різних напрямках, а саме: обмін інформацією (приймання-передача, обробка і зберігання команд, сигналів, розпоряджень, бойових документів); обробка та зберігання інформації (електронний документообіг, ведення баз даних, обробка і зберігання даних поточної обстановки); інформаційно-розрахунковий (організація управління, взаємодії та рекогносцировки на місцевості; збір, обробка та облік даних про свої війська, противника та фізико-географічні умови; оцінка обстановки; підтримка вироблення замислу; планування бою (бойових дій); планування матеріально-технічного забезпечення; управління підрозділами в надзвичайних ситуація техногенного та природного характеру; управління артилерією та артилерійськими підрозділами ін.); картографічна підтримка (вирішення геоінформаційних завдань); навігаційна підтримка (безперервне визначення значень навігаційних параметрів наземних рухомих об'єктів).

Пилипчук Ю.В. (НЦЗІ ВІТІ)
Петров Д.В. (НЦЗІ ВІТІ)
Остапук А.І. (НЦЗІ ВІТІ)
Гетьман А.В. (НЦЗІ ВІТІ)

СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ ІНФОРМАЦІЙНИХ СИСТЕМ В ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Актуальність. На сьогодні у сучасних конфліктах одною з важливіших складових війн є інформаційне протиборство. З'являються нові види озброєння, засновані на застосуванні інформаційних технологій, розвиваються засоби розвідки, автоматизовані системи управління військами та зброєю.

Одним із пріоритетних завдань оборонної реформи є створення ефективної системи управління Збройними силами України, як основи системи управління силами оборони держави. Одночасно з реалізацією заходів, пов'язаних з безпосереднім реформуванням оборонного відомства, важливу роль у реалізації цього завдання відіграватимуть упровадження в діяльність органів управління та військ (сил) сучасних інформаційних технологій, адаптація найкращих практик та стандартів провідних країн – членів НАТО, комплексна автоматизація процесів оперативного (бойового) управління, зв'язку, розвідки та спостереження (C4ISR), обліку та управління оборонними ресурсами (DRMIS).

Викладення основного матеріалу. Автоматизація повинна охопити такі функції, як доведення команд і розпоряджень, контроль за їх виконанням; відображення оперативної обстановки з використанням цифрових карт і геоінформаційних даних; обробку та зберігання інформації; захищений обмін електронними даними – як текстовими, так і графічними – в автоматизованому режимі; проведення оперативно-тактичних розрахунків, імітаційного моделювання задач з застосування підрозділів Збройних Сил. Це неповний перелік того, що має вирішуватися в рамках поставленого ключового завдання.

Водночас, ці наміри підтверджуються положеннями, викладеними в Указі Президента України "Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року "Про Стратегічний оборонний бюлетень України" [2], а саме, у другому розділі, який присвячений системі управління силами оборони. У ньому йдеться про створення до 2020 року національної телекомунікаційної мережі, модернізації та переведення на сучасні цифрові технології системи спеціального зв'язку, відомчих інформаційно-комунікаційних мереж та систем зв'язку пунктів управління органів державної влади, а також створення автоматизованої системи C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) складових сил оборони, яка відповідає стандартам, доктринам і рекомендаціям НАТО на всіх рівнях управління (тактичному, оперативному та стратегічному) із визначеною специфікою базових можливостей. У Бюлетені також наголошено на врахуванні сумісності системи управління військами і зброєю із системами ресурсного забезпечення.

На теперішній час практично відсутня комплексна автоматизація основних процесів управління ЗСУ, низька ефективність управління оборонними ресурсами та низький рівень існуючої інформаційної інфраструктури щодо забезпечення військового керівництва та органів військового управління інформаційно-аналітичною складовою для підтримки прийняття рішень у сфері управління оборонними ресурсами, не повною мірою узгоджено між собою розробки, що ведуться на їх замовлення. Розробляються та використовуються окремі інформаційні (автоматизовані) системи, які не становлять єдиної системи, питання технічної та інформаційної сумісності здебільшого не вирішуються, що в майбутньому неминуче призведе до проблем інтеграції розробок.

Крім того, за напрямом управління оборонними ресурсами створені окремі компоненти інформаційної інфраструктури та інформаційних систем, які різняться між

собою за часом створення, ступенем завершеності, масштабом розгортання та використаними технологіями, обсягом охоплених процесів та наповненими даними.

Незважаючи на тривалий термін існування завдання щодо створення ЄАСУ ЗСУ як матеріально-технічної основи системи управління ЗСУ та силами оборони держави, значний обсяг виділених на це фінансових та інших ресурсів, у цілому завдання залишається невиконаним.

Відповідно до Концепції відомчих програм створення ЄАСУ ЗСУ, єдиної інформаційної системи управління оборонними ресурсами та інформаційної інфраструктури на період до 2020 року найбільш раціональним варіантом створення Єдиної автоматизованої системи ЗСУ є варіант створення першочергових базових складових ЄАСУ ЗСУ, які повинні утворювати закінчені вертикалі співпідпорядкованих об'єктів управління відповідного функціонального призначення від стратегічного до тактичного рівня за основними напрямами діяльності Збройних Сил з підготовки, планування, застосування військ (сил) та їх всебічного забезпечення.

Відповідно до технологічних особливостей, у першу чергу, необхідно розробити та прийняти на озброєння пусковий комплекс ЄАСУ ЗСУ у складі дослідного району, що повинен охоплювати всі рівні управління ЗС, мати обмежену функціональність та обов'язково включати:

розробку ядра системи як для стаціонарної, так і для мобільної компоненти;

розробку базових сервісів для всіх рівнів управління та типів програмно-апаратних платформ;

створення єдиного інформаційного простору в межах дослідного району з інтеграцією до нього прийнятих на озброєння (розроблених), розроблюваних автоматизованих систем;

спеціального програмного забезпечення масового використання, а саме оповіщення, ведення комплексної обстановки, електронного документообігу, цифрового підпису.

При цьому мають бути реалізовані мінімально необхідні функціональні можливості по всій вертикалі системи управління ЗС та можливе використання існуючих типових і уніфікованих засобів автоматизації, зв'язку, телекомунікацій закордонних виробників, що мають атестати відповідності щодо можливості використання та забезпечення захисту інформації відповідно до вимог нормативних документів системи технічного та криптографічного захисту інформації в Україні.

Реалізація зазначеного варіанта дасть можливість скоротити терміни створення, заощадити ресурси та еволюційно нарощувати складові ЄАСУ ЗСУ щодо безпосередньо військово-політичного, бойового та адміністративно-господарського напрямів ЗС.

C4ISR ЗС України будується у відповідності до прийнятої в країнах НАТО мережецентричної концепції управління військами в ході ведення бойових дій.

Архітектура C4ISR означає підхід, який передбачає комплексну інтеграцію засобів оперативно-стратегічної розвідки, спостереження та військової розвідки (Intelligence, urveillance and Reconnaissance) із системами управління, контролю, зв'язку та обчислювальними засобами (Command, Control, Communication, Computers) в єдиному інформаційному середовищі, яке, у свою чергу, забезпечує інтеграцію навігаційної, загальногеографічної та тактичної інформації в єдиній географічній системі координат. Разом перелічені інтеграційні процеси дають змогу реалізовувати мережецентричну архітектуру управління військами, яка у деякій мірі змінила підходи до ведення бойових дій за рахунок використання принципів мережецентричності.

C4ISR також розуміють як єдиний масштабний програмно-технічний комплекс. У назві C4ISR (командування, контроль, зв'язок, комп'ютери, розвідка, спостереження, рекогносцировка) перераховані функції, які мають бути автоматизованими. Тому системи, побудовані за подібною концепцією, носять назву інтегрованих систем розвідки та управління.

На відміну від C2+ або C2SR (Command, Control, Surveillance, Reconnaissance) – концепції тактичного рівня, де самостійною одиницею є окремий солдат чи військова техніка, у C4ISR ці одиниці стають членами тактичної мережі або бойового інтернету.

Архітектури та концепції C4ISR і C2+ передбачають створення інформаційного середовища, яке дає змогу:

автоматично визначати положення і переміщення своїх підрозділів (автоматично відображається на електронних картах);

автоматично визначати положення противника і його переміщення (також відображається на електронних картах);

автоматично обирати маршрути руху;

автоматично давати цілевказівки засобам вогневого ураження;

автоматично інформувати свої підрозділи про дії і місцезнаходження їх сусідів і противника.

Ці можливості доступні на оперативному і тактичному рівнях. До зазначених пунктів для C4ISR, тобто оперативного рівня, слід додати:

повна автоматизація збору інформації та її обробка;

автоматизоване надання варіантів рішення командира, заснованих на автоматично отриманих розвідданих, а також на інформації про сили і засоби, що є в розпорядженні;

моделювання бою і його можливих результатів;

пропозиції часткових рішень для командира в ході бою, засновані на поточній ситуації.

Таким чином, різниця між тактичним і оперативним рівнями систем полягає в можливості автоматизації прийняття рішення, моделюванні бою і прогнозуванні результатів.

Крім того, C4ISR має розширену автоматизацію для логістики. Облік витрат необхідних засобів системою ведеться постійно.

На сьогодні концепція C4ISR є найбільш складною з існуючих у світі, а в класичному (повному) вигляді реалізована лише у збройних силах США та КНР. Окремі елементи концепції впроваджені у ЗС провідних країн НАТО – Великобританії, Франції та ФРН. Після вступу до НАТО програми створення таких систем започаткували Польща та Румунія, але їх завершення очікується не раніше 2025 – 2030 років.

Платформою, що виступає в ролі шлюзу між підсистемами спеціального призначення та вирішує задачу інтеграції у автоматизовану систему *C4ISR* компонентів сил оборони НАТО, виступає система „Дельта”.

Згідно наказу Генерального штабу Збройних сил України № 78 від 06.03.2017 та з метою проведення інтеграції автоматизованих (інформаційних, інформаційно-телекомунікаційних) систем Збройних сил України, підвищення ефективності управління Збройних сил України, регламентування порядку розгортання та використання інтеграційної платформи Збройних сил України „Дельта” затверджується Тимчасове положення про порядок використання інтеграційної платформи Збройних сил України „Дельта”

Це Тимчасове положення визначає призначення та мету створення, основні завдання, склад, особливості функціонування, відповідальність за організацію розгортання та використання інтеграційної платформи Збройних сил України „Дельта” (далі – „Дельта”).

„Дельта” – це програмна платформа, яка призначена для інтеграції інформаційних ресурсів різнотипних інформаційних та автоматизованих систем, створення єдиного геоінформацІйного та інформаційно-аналітичного середовища органів військового управління, військових частин та підрозділів Збройних сил України з розмежуванням прав доступу користувачів до цих ресурсів.

Метою створення „Дельта” є забезпечення інформаційної взаємодії та сумісності між системами різного функціонального призначення, побудованими на різних програмно-апаратних платформах із застосуванням широкого спектру інформаційних технологій та

геоінформаційних платформ, у тому числі застарілих, за рахунок застосування єдиного протоколу інформаційного обміну, який прийнято у країнах-членах НАТО.

Висновок. Отже, відповідно до Концепції відомчих програм створення ЄАСУ ЗСУ, єдиної інформаційної системи управління оборонними ресурсами та інформаційної інфраструктури на період до 2020 року та з урахуванням особливостей оборонного планування на основі спроможностей, найбільш раціональними шляхами та способами розв'язання проблеми створення ЄАСУ, єдиної інформаційної системи управління оборонними ресурсами та інформаційної інфраструктури необхідно вважати:

формування та удосконалення нормативно-правової бази з питань створення, впровадження, експлуатації, супроводження ЄАСУ ЗСУ, єдиної інформаційної системи управління оборонними ресурсами та інформаційної інфраструктури;

створення системи взаємопов'язаних організаційних структур, відповідальних за повний життєвий цикл системи;

удосконалення системи підготовки фахівців з питань застосування та експлуатації інформаційних (автоматизованих) систем військового призначення;

розробка (закупівля) та впровадження комплексів засобів автоматизації (програмно-технічних комплексів) автоматизованих систем різного функціонального призначення;

розробка уніфікованих програмно-технічних платформ та спеціального програмного забезпечення;

можливість розвитку та модернізації за рахунок ведення нових функціональних систем (сервісів), розширення функцій створених систем, підключення нових інформаційних ресурсів та розширення кола користувачів;

розвиток інформаційної інфраструктури в інтересах створення ЄАСУ ЗСУ та її складових;

формування єдиних правил, політик і стандартів технічної та інформаційної сумісності інформаційних (автоматизованих) систем та їх компонентів, у тому числі врахування стандартів НАТО щодо побудови та розвитку комунікаційних та інформаційних систем.

ЛІТЕРАТУРА:

1. Концепція відомчих створення Єдиної автоматизованої системи управління Збройними силами України, єдиної інформаційної системи управління оборонними ресурсами та інформаційної інфраструктури на період до 2020 року затвердженая Міністром оборони України від 12 травня 2018 року.

2. План дій щодо впровадження оборонної реформи у 2016 – 2020 роках (дорожня карта оборонної реформи).

3. Указ Президента України від 06.06.2016 року№ 240/2016 „Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року "Про Стратегічний оборонний бюлетень України".

4. Артюх В. М. Современный этап разработки и строительства Единой автоматизированной системы управления Вооруженными Силами Украины / В. М. Артюх, В. К. Медведев // Оборонный вестник. – 2012. – № 1. – С. 15 – 24.

5. Галаган В.І., Сурков О.О.,Прокопенко О.С. Аналіз впровадження автоматизованих систем управління військами (силами) в провідних країн світу // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України. – К.: ЦВСД НУОА, 2013. – № 3 (49). – С. 40 – 46.

6. Пащетник О.Д. Аналіз світових тенденцій розвитку автоматизованих систем управління військами і зброєю // Наука і техніка Повітряних Сил Збройних сил України. – 2015. – № 2 (19). – С. 64 – 68.

7. Золотова І.Г. Стан та перспективи розвитку автоматизованих систем управління військами (зброєю) передових країн світу / І.Г. Золотова, М.Ю. Голобородько, О.В. Поривай // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України. – К.: ЦВСД НУОА, 2013. – № 2 (48). – С. 33 – 36.

к.т.н. Пилипчук В.В. (ВДА імені Є. Березняка)

МЕТОД ВИЯВЛЕННЯ РУХОМИХ МОРСЬКИХ ОБ'ЄКТІВ НА ЦИФРОВИХ ЗНІМКАХ ВИДОВИХ ЗАСОБІВ

Морською доктриною України на період до 2035 року передбачено, що для розв'язання завдань, які покладаються на Військово-Морські Сили та Морську охорону Держприкордонслужби, необхідно забезпечити, зокрема, створення засобів виявлення та ураження надводних та підводних цілей. Потреба у вирішенні цього надзвичайно актуального питання нещодавно підтверджена Розпорядженням Кабміну України від 13 жовтня 2015 року № 1068-р „Про затвердження плану першочергових заходів з облаштування державного кордону вздовж берегової лінії та забезпечення охорони територіального моря України в межах Донецької, Запорізької, Херсонської та Миколаївської областей, тобто необхідним є створення системи засобів виявлення морських об'єктів.

Сучасні засоби виявлення морських об'єктів включають:

– гідроакустичні засоби (гідроакустичні станції та радіогідроакустичні буйкові станції);

– магнітометричні засоби;

– видові засоби (оптико-електронні прилади, тепловізійна апаратура, лазерні системи, радіолокатори із синтезованою апертурою (РСА).

Низька ефективність використання систем на основі перших двох видів засобів обумовлюється високою мінливість ознак які залишають морські об'єкти. Наприклад, магнітні аномалії досить швидко зглажуться з відстанню, що обмежує можливості магнітометричного способу виявлення ПЧ радіусом до 1…3 миль. Тому актуальним є створення системи засобів виявлення морських об'єктів якій буде ґрунтуватись на виявленні основних демаскуючих ознак морських рухомих об'єктів (теплових кільватерних слідів, турбулентних слідів, корабельних хвиль) які комплексно будуть реєструватись видовими засобами.

Відомо, що об'єкт, який рухається на поверхні чи у водному середовищі, викликає його турбулентне збурювання, що може приводити до змішування різних температурних шарів води й піднімання їх на поверхню. Це збурення свідчить про присутність рухомого об'єкта та може бути помічений із супутника або літака за змінами у параметрах поверхні моря. Зокрема, експериментально встановлено, що на морській поверхні після проходження зануреного об'єкта утворюється температурний слід з контрастом стосовно фону в 0,5°С, який зберігається протягом 5…6 годин.

Крім зазначеного морський рухомий об'єкт може залишати збурювання у вигляді сукупності дрібних хвиль (брижей). По спектру брижі можливо визначати характер руху об'єкту та певні його параметри (швидкість, напрям).

В роботі пропонується метод визначення морських рухомих об'єктів за знімками отриманими від оптико-електронних та радіолокаційних засобів. Він передбачає наступні етапи:

попереднє оброблення знімків,

вибір розрахункової ділянки та установка параметрів пошуку,

визначення ознак детектування (координат и напрямку руху об'єкта, швидкості руху об'єкта),

розпізнавання морського об'єкта (базується на алгоритмах та методах контурного аналізу) та інтерпретування сцени.

Подальші дослідження варто спрямувати на накопичення статистики вимірювань параметрів руху морських об'єктів для формування еталонної бази морських об'єктів.

Півторайко І. В. (НУБіП України)
д. т. н. Лахно В. А. (НУБіП України)

ВИЯВЛЕННЯ АНОМАЛІЙ ЗА ДОПОМОГОЮ ЗОВНІШНЬОГО (OUTLIER) ПІДХОДУ

Актуальність. Завдяки високому використанню Інтернету в нашому сьогоднішньому житті, безпека мережі стала ключовою основою будь-якої веб-програми: інтернет-аукціони, роздрібні продажі в Інтернеті тощо. Системи виявлення вторгнень намагаються виявити атаки на цільові системи шляхом вивчення різних записів інформації, що спостерігаються в мережевих процесах [1]. Це може розглядатися як один із важливих способів ефективного вирішення проблем безпеки мережі.

Мета. Здійснити аналіз основних загроз мережі та систем виявлення вторгнень.

Виклад основного матеріалу

Вторгнення в Інтернет може поставити під загрозу безпеку даних за допомогою кількох засобів. У наш час швидко зростаючі масштаби мереж, швидкість передачі даних та непередбачуване використання Інтернету додали ще більше проблем з аномаліями. Таким чином, дослідникам необхідно розробити більш надійні, ефективні системи самоконтролю, які б впорядковували непередбачувані ситуації та мали можливість виконувати операції, позбавлені людської взаємодії. Стабільність виявлення та точність виявлення – два ключових показники, які використовуються для оцінки IDS (Система виявлення вторгнень) [2]. Багато досліджень IDS було проведено для покращення стабільності та виявлення точність [3].

Класифікація систем виявлення вторгнень (ІДС) Класифікація є одним з найбільш відомих підходів до рішення проблеми описаної вище. Організація Національного інституту стандартів та технологій (NIST) надає керівний документ щодо систем виявлення вторгнень. Система виявлення вторгнень коротко класифікується на три різні категорії:

IDS на основі хоста;

IDS на основі мережі;

IDS оцінки вразливості.

На рис. 1 наведена типова архітуктура системи виявлення вторгнень.

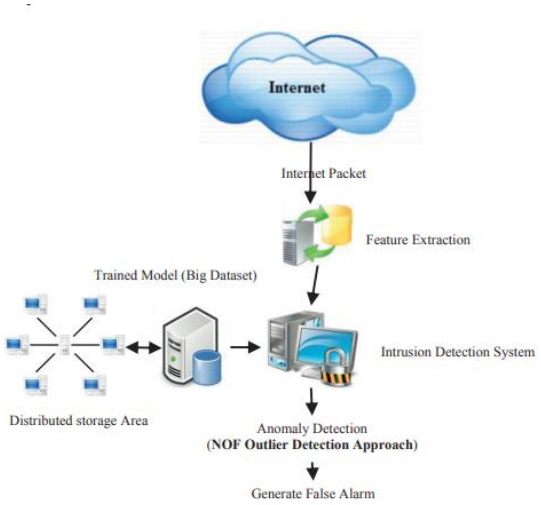


Рис. 1. Типова архітуктура системи виявлення вторгнень

Зовнішній підхід до виявлення вторгнень. Нормальні об’єкти даних мають щільне сусідство, тоді як „сторонні”, далеко не сусіди. Сторонні об’єкти – це об’єкти зовнішніх шарів. Основна ідея цього підходу полягає в тому, щоб призначити приклад даних ступеню, який називається стороннім коефіцієнтом сусідства (NOF) та знайти рідкісні дані, поведінка

яких є надзвичайно винятковою у порівнянні з великою кількістю звичайних даних. Етапи алгоритму, які використовуються для обчислення NOF для всіх прикладів даних, є такими:

1. Для кожного прикладу даних O обчислюється k-відстань – найближче сусідство (де всі точки в k-відстані утворюють сферу).
2. Далі знаходиться відстань досяжності для кожного прикладу даних O відносно прикладу даних p як: відстань (O, p) = max {k-відстань (p), d (O, p)}, де d (O, p) - відстань між прикладом даних O і прикладом даних p.
3. Потім обчислюється локальна щільність досяжності для кожного прикладу даних O, обернена середня відстань доступності базується на прикладі даних MinPts (мінімальна кількість об'єктів) O та найближчих сусідів.
4. Знаходиться NOF для всіх прикладів даних O як середнє значення прикладу даних щодо коефіцієнтів локальної щільності локальної доступності та локальної щільності досягнення найближчих сусідів OO.

Переваги запропонованого підходу NOF – кластери формально визначаються як максимальні набори об'єктів, пов'язаних з щільністю. На рис. 2 представлене візуальне розміщення об'єктів моніторингу NOF.

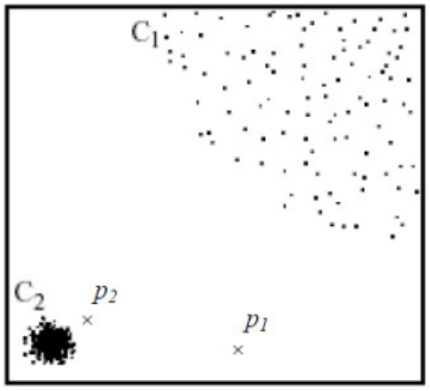


Рис. 2. NOF підхід до виявлення аномалій

Висновки

У наш час швидко зростаючі масштаби мереж, швидкість передачі даних та непередбачуване використання Інтернету додали ще більше проблем з аномаліями. Основна ідея цього підходу полягає в тому, щоб призначити приклад даних ступеню, який називається стороннім коефіцієнтом сусідства (NOF) та знайти рідкісні дані, поведінка яких є надзвичайно винятковою у порівнянні з великою кількістю звичайних даних.

ЛІТЕРАТУРА

1. Planquart, J. P. (2001). Стаття, Застосування нейронних мереж до виявлення вторгнень, Інститут ДАНС .1 – 3.
2. Shah, K., Dave, N., Chavan, S., Mukherjee, S., Abraham, A., Sanyal S. Адаптивна нейро-нечітка система виявлення вторгнень. Міжнародна конференція IEEE з інформаційних технологій: кодування та обчислення (ITCC'04), т. 1. США: IEEE Computer Society; 2004; 70 –74.
3. Silva, L. D. S., Santos, A. C., Mancilha, T. D., Silva, J. D., Montes, A. Виявлення шаблонів атаки в реальному мережевому трафіку з ANNIDA. Експертні системи з додатками, 34 (4); 2008; 2326 – 2333.

к.т.н. Погребняк Л.М. (ВІТІ)
к.т.н. Кононова І.В. (НТУУ „КПІ ”)

ЕФЕКТИВНІСТЬ ЗАВАДОСТІЙКОГО ТА ПРОСТОРОВОГО КОДУВАНЬ В НЕСТАЦІОНАРНИХ ЧАСТОТНО-СЕЛЕКТИВНИХ КАНАЛАХ СИСТЕМ ВІЙСЬКОВОГО РАДІОЗВ'ЯЗКУ

Внаслідок особливостей дислокації та динамічного переміщення органів та пунктів військового управління канали системи військового радіозв'язку (СВРЗ) характеризуються високими рівнями нестаціонарності та частотної селективності. Враховуючи складну структуру швидких частотно-селективних завмирань та обмеженість частотно-енергетичного ресурсу каналів військового радіозв'язку, передача великих обсягів інформації потребує розробки високошвидкісних завадостійких сигнальнокодових конструкцій для ефективного (близьке до теоретичних меж) використання пропускної спроможності реальних каналів.

Аналіз наукових робіт показав, що незважаючи на високу коректуючу здатність завадостійких канальних кодів їх застосування у нестаціонарних частотно-селективних каналах є низькоефективним.

Тому необхідно проведення досліджень для підвищення енергетичної ефективності системи передачі за рахунок сумісного застосування типових завадостійких кодів та методів просторового кодування з підвищеною стійкістю до нестаціонарності і частотної селективності. Аналіз методів просторового кодування показав, що в частотно-селективних каналах з помірним рівнем нестаціонарності найбільш ефективним є метод *WHSTCC*, який базується на алгоритмі просторово-часового блочного кодування (*STBC*) та реалізує схему спряженої компенсації (*conjugate cancellation, CC*) міжканальних завад і максимальне обмеження кількості піднесучих *OFDM* з одночасним посиленням частотного рознесення сигналів кодером Уолша-Адамара (*Walsh-Hadamard*, WH). Але при нормованому значені доплерівського зсуву частоти, яке перевищує 0,1 ефективність методу *WHSTCC* суттєво знижується, що є результатом неоптимальної роботи схеми *CC*. За таких умов доцільно використовувати метод просторово-частотного кодування (*SF*). Метод *SF* ґрунтується на застосуванні короткого унітарного перетворення Уолша-Адамара (2×2) до вихідних символів *SFBC* кодера Аламоуті. Таке перетворення забезпечує прийом сигналів сусідніх підканалів після зворотної процедури *WH* з однаковим коефіцієнтом передачі, що по суті еквівалентно перетворенню частотно-селективного каналу в канал з кусочно-плоскою амплітудночастотною характеристикою на всіх або частині суміжних пар підканалів *OFDM* в залежності від ансамбля модуляційних сигналів. Проведений аналіз ефективності основних завадостійких кодів у каналах систем військового радіозв'язку з помірною нестаціонарністю показав, що енергетичний виграш при сумісному застосуванні удосконалених методів просторового кодування та згорточного турбокоду (в залежності від об'єму ансамблю сигналів) становить 5,0 – 6,0 дБ. Застосування завадостійкого коду дозволяє суттєво підвищити (більш ніж у два рази) стійкість СВРЗ до нестаціонарності каналу, а також збільшити допустимі значення величини нормованого доплерівського зсуву. В частотно-селективних каналах з високими рівнями нестаціонарності базовий метод просторово-частотного кодування навіть сумісно з завадостійкими кодами не забезпечує необхідну достовірність передачі інформації. Це пов'язано з суттєвою залежністю методу *SFBC* від частотної селективності каналу. В тож же час його удосконалена версія враховує вказану критичність та разом із згорточним турбокодом збільшує енергетичну ефективність СВРЗ в залежності від об'єму ансамбля сигналів на 4 – 7 дБ (*BPSK*) та 3,8 – 4,2 дБ (*QPSK*). В цілому стійкість СВРЗ до нестаціонарності за рахунок канального кодування підвищується на 20 – 25 % (*BPSK*) та 50 – 87 % (*QPSK*).

Напрямом подальших досліджень є узгодження завадостійкого кодування з методами адаптивної модуляції і просторового кодування в рамках єдиної сигнально-кодової конструкції, що може забезпечити високоефективне використання енергетичного, частотного та просторового ресурсів реальних безпроводових каналів зв'язку.

к.т.н. Подліпаєв В.О. (ІІТГІП)
к.т.н. Хижняк І.А. (ХНУПС ім. Івана Кожедуба)

АНАЛІЗ СУЧАСНИХ ГЕОІНФОРМАЦІЙНИХ СИСТЕМ ЩОДО ТРАНСДИСЦИПЛІНАРНОГО ВИКОРИСТАННЯ СЛАБОСТРУКТУРОВАНИХ ДАНИХ

Відомо, що геопросторова інформація в сучасних умовах стала важливим стратегічним ресурсом державного управління та вагомим чинником сталого соціально-економічного розвитку країни. Потреба у геоінформаційних технологіях у багатьох сферах діяльності держави, говорить про їх актуальність.

Одним з основних та найбільш потужним аналітичним елементом геоінформаційні підтримці є геопросторовий аналіз. Геопросторовий аналіз [1] – це динамічний процес роботи зі значними обсягами даних. Причому, не зважаючи на те, що аналіз називається геопросторовий, в основному опрацьовуються не геопросторові дані, а інша інформація, яка безпосередньо пов'язана з ними або має контекстне відношення до них.

Всі необхідні для геопросторового аналізу дані та пов'язану з ними інформацію, експерт не виробляє. Однак, всі ці дані йому потрібні постійно і як можна оперативніше. А вони виробляються та знаходяться на різноманітних інформаційних ресурсах, які відносяться до різних сфер знань. Проблематики додає й той факт, що вона зберігається в неструктурованому або слабоструктурованому вигляді.

Таким чином виникає наступна актуальна наукова задача – визначення відповідної геоінформаційної системи (ГІС), яка відповідає достатнім вимогам щодо пошуку, оброблення та використання геопросторових даних і пов'язаної з ними інформації з різнорідних інформаційних ресурсів, а також ведення трансдисциплінарного геопросторового аналізу в процесі вирішення складних прикладних задач, які характеризуються високою міждисциплінарністю.

На сьогоднішній день у світі є велика кількість програмних реалізацій ГІС [2-5]:

ГІС-платформи ArcGIS від компанії ESRI і MapInfo від компанії MapInfo Corp;

лінійка програмних продуктів MGE, GeoMedia / GeoMedia Pro від компанії Integraph і AutoCAD Map, AutoCAD Civil, MapGuide від компанії Autodesk Inc;

CMaps Analytics від американської компанії Centigon Solutions;

пакет програмних продуктів MicroStation від компанії Bentley Systems;

Digital від української компанії GeoSystem.

Також існують інші менш популярні комерційні ГІС.

На достатньо потужному функціональному рівні знаходяться ГІС, які побудовані на відкритому програмному забезпечені [6-8]: Quantum GIS, GRASS GIS та інші.

За своїм функціоналом наведені відкриті ГІС на достойному рівні конкурують з комерційними аналогами. Відкриті ГІС розвиваються та постійно оновлюються, про що свідчить наявність у мережі інсталяційних версій та достатня частота їх оновлення. Архітектурі відкритих ГІС також характерна багаторівнева модульна структура.

У більшості відкритих ГІС є функції читання та запису (редагування) географічних та просторових даних, а також часових характеристик і атрибутів.

Неможливо залишити поза увагою наявність достатнього розмаїття онлайн-сервісів потужних Web-картографічних або ГІС-порталів (ArcGIS Online, Google Earth, Google Maps, Wikimapia, Bing Maps, MapQuest, Yahoo! Maps, MultiMap.com, Map24.com, Expedia.com, MapsOnUS тощо) [9]. Подібні Web-сервіси, окрім базових функцій ГІС, містять різноманітні геопросторові дані по певним територіям.

Для порівняння існуючих ГІС були вибрані певні параметри:

робота з неструктурованими або слабоструктурованими даними, які знаходяться в різноманітних інформаційних ресурсах, без переміщення змісту цих ресурсів до баз даних самої ГІС;

тематична (критеріальна) систематизація знайденої інформації;

наявність веб-орієнтованих засобів її представлення;

можливість роботи з різними форматами геопросторових даних та пов’язаної з ними інформації.

При всьому арсеналі інструментарію, операційних алгоритмів, реалізації аналітичних методів, які є у досліджених ГІС, онтологічний підхід [10] щодо трансдисциплінарного використання геопросторових даних та пов’язаної з ними інформацією не реалізований. Що приводить до використання складних алгоритмів пошуку та збору потрібної інформації з різних інформаційних ресурсів та проведення тематичної систематизації зібраних даних.

Дослідження проблем, пов’язаних з організацією ефективного інформаційного забезпечення геопросторового аналізу міждисциплінарних інформаційних ресурсів, показує, що існує необхідність розробки нових методів та засобів управління інформацією для забезпечення доступу до знань, їх об’єднання та формування нових знань [11].

Це питання набуває найбільшої актуальності коли необхідно знайти не геопросторові дані, а саме пов’язану з ними інформацію, які знаходяться в різних інформаційних ресурсах. А якщо інформація в цих ресурсах викладена та зберігається у неструктурованому або слабоструктурованому вигляді, то проблематика значно загострюється.

Тому розв’язання задачі забезпечення інформаційного забезпечення геопросторового аналізу полягає в інтеграції або поєднання міждисциплінарного інформаційного середовища з геоінформаційною системою та в необхідності розробки засобів забезпечення загального трансдисциплінарного онтологічного представлення семантики, що забезпечить можливості зберігання, обробки та доступу до його різнорідних об’єктів та інформаційних одиниць.

ЛІТЕРАТУРА

1. Митчелл Энди. Руководство по ГИС анализу. Часть 1 : Пространственные модели и взаимосвязи / Энди Митчелл ; пер. с англ. – К., ЗАО ЕСОММ Со ; Стилос, 2000. – 198 с.

2. Курочкін В. М. Аналіз та перспективи розвитку сучасних геоінформаційних рішень для оптимізації ведення сільського господарства / В. М. Курочкін // Проблеми інформатизації та управління. – 2015. – № 4 (52). – С. 75 – 81.

3. Esri: GIS Mapping Software, Spatial Data Analytics & Location Platform. [Electronic resourse]. Режим доступу: URL: https://www.esri.com/en-us/home.

4. Web-сайт корпорації MapInfo [Electronic resourse]. Режим доступу: http://www.mapinfo. com/.

5. Руководство по Autodesk Civil 2008. Web-сайт Autodesk [Electronic resourse]. Режим доступу: www.autodesk.com.

6. Open-Source Software (OSS). [Electronic resourse]. Available: https://www.techopedia.com/definition/5602/open-source-software-oss. Accessed on: August 03, 2018.

7. Зінов’єва І. С. Використання відкритих геоінформаційних систем у підготовці фахівців з комп'ютерних наук / І. С. Зінов’єва // Інформаційні технології і засоби навчання. – 2018. – № 68 (6).

8. QGIS The Leading Open Source Desktop GIS [Електронний ресурс]. Режим доступу: http://www.qgis.org/.

9. Павленко Л. А. Геоінформаційні системи : навчальний посібник / Л. А. Павленко. – Х. : Вид. ХНЕУ, 2013. – 260 с.

10. Стрижак А.Е. Онтологические аспекты трансдисциплинарной интеграции информационных ресурсов / А. Е. Стрижак // Открытые информационные и компьютерные интегрированные технологии. – 2014. – № 65. – С. 211 – 223.

11. Stryzhak O., Prychodniuk V., Podlipaiev V. (2019) Model of Transdisciplinary Representation of GEOspatial Information. In: Ilchenko M., Uryvsky L., Globa L. (eds) Advances in Information and Communication Technologies. UKRMICO 2018. Lecture Notes in Electrical Engineering, vol 560. Springer, Cham, pp.34 – 72.

Покотилюк О.О. (ВІТІ)
Стоцький І.В. (ВІТІ)

ПРОГРАМНИЙ МОДУЛЬ ОБРАХУНКУ МОЖЛИВИХ НАСЛІДКІВ ЯДЕРНОГО ВИБУХУ

Для розрахунків можливих наслідків ядерних вибухів у провідних країнах світу і в країнах які входять у склад НАТО використовуються програмні модулі, які автоматично розраховують і виводять всі можливі наслідки ядерних зарядів будь-якої потужності. В збройних силах нашої країни для розрахунків можливих наслідків ядерного вибуху використовують застарілі, неактуальні на сьогоднішній день, розрахункові лінійки (розрахункова лінійка «РЛ», яка використовується для оцінки радіаційної обстановки при наземних вибухах, розрахункова лінійка «РИЛ-2», яка використовується для оцінки втрат особового складу при наземному вибуху). Розрахунок даними лінійками здійснюється вручну. Щоб здійснити розрахунки даними лінійками, потрібно витрати велику кількість часу. **Метою** даної роботи є дослідження принципу використання розрахункових лінійок та створення програмного модуля, який їх замінить. Для створення програмного модуля використане середовище розробки *Android Studio*, що в свою чергу зробить його доступним, так як технічні вимоги не є високими. Створений швидкий алгоритм обрахунків даних, для зручного і швидкого обрахунку даних. Створена математична модель, у математичній моделі частково задіяні сталі значення, які зображені у вигляді таблиць. Збереження табличних даних відбувається у *Microsoft Excel.* Зчитування табличних даних з *Microsoft Excel* виконується за допомогою відповідного *application programming interface „Aspose.Cells for Java”* який, у свою чергу, дозволяє читати, записувати і маніпулювати таблицею.

Математична модель розрахункової лінійки, яка використовується для оцінки радіаційної обстановки при наземних вибухах включає в себе:

– визначення можливих доз опромінення отриманих особовим складом при діях на забрудненій радіацією місцевості (1):

$$A = (P_{ср} * t) / K \quad (1)$$

де значення *Pcp* – середнє арифметичне значення рівня радіації, *t* – час перебування у зоні ураження, *K* – коефіцієнт ослаблення;

– визначення доз опромінення які отримає особовий склад підрозділу під час здійснення маршу у зоні радіаційного зараження (2):

$$A = (P_{\max} * e) / 4UK, \; A = (P_{ср} * e) / UK \quad (2)$$

де значення *Pmax* – середнє арифметичне значення рівня радіації, *e* – довжина зараженого шляху, *U* – швидкість руху, *K* – коефіцієнт ослаблення;

– вираховування впливу місцевих умов на дози опромінення (3):

$$D_M = K_M * D \quad (3)$$

де значення виступає *Км* – коефіцієнт спадання доз, в належності від місцевості, *D* – коефіцієнт захисту (табличні дані).

– здійснення розрахунку розповсюдження радіаційної хмари (4):

$$P = (v * q) / h \quad (4)$$

де *v* – швидкість вітру, *q* – потужність заряду, *h* – висота або глибина в залежності від виду вибуху.

Висновки. Таким чином, створений програмний модуль дозволить автоматизувати процес здійснення розрахунків можливих наслідків ядерного вибуху, виведе збройні сили України на рівень провідних країн світу та країн які входять у склад НАТО, які мають відповідне програмне забезпечення. Використання програмного модулю обрахунків можливих наслідків ядерного вибуху дозволяє вдосконалити управлінську діяльність і може бути використаною в експертних системах, а також в системах підтримки прийняття рішення.

Поліський О.М.
військова частина А1906

МЕТОДИКА ФІЛЬТРАЦІЇ ОЦІНОК ЕЛЕМЕНТІВ ВЕКТОРУ СТАНУ ПРИ УМОВІ РІВНОМІРНОГО ПРЯМОЛІНІЙНОГО РУХУ ЦІЛІ

В сучасних умовах система ППО є основним стримуючим фактором широкомасштабної збройної агресії Російської Федерації в зоні проведення ООС і повинна відповідати сучасним вимогам ведення збройної боротьби в повітрі.

Станції радіолокаційної розвідки хоча й мають змогу виявити аеродинамічні цілі противника на достатніх відстанях, але мають ряд проблем з супроводом деяких з них, насамперед винищувачів та крилатих ракет, оскільки ті мають великі швидкісні і маневрені показники, через що засоби автоматизації мають низку проблем, пов'язаних з визначенням їх траєкторії та подальшим супроводом, що в свою чергу зменшує можливість засобів ППО знищити ці цілі в разі необхідності.

Для вирішення питання супроводження траєкторії необхідно мати певний апарат, за допомогою якого засоби та комплекси автоматизації будуть виконувати цю функцію. На даний момент існує багато методик для виконання поставленої задачі. Як відомо, для отримання траєкторії цілі необхідно на основі отриманих результатів спостереження передбачити наступне положення цілі, тобто екстраполювати отримані данні.

Оскільки при розвідці повітряного простору засобами РТВ мають місце похибки вимірювання, а при подальшій їх обробці засобами автоматизації - похибки екстраполяції, то для зменшення їх значень необхідно реалізувати процедури згладжування дискретних параметрів траєкторії. Ці процедури дають змогу суттєво зменшити ці похибки в умовах ,,управління" моделлю руху засобу повітряного нападу противника.

При дослідженні цього питання нам відомо, що джерело - радіолокаційна інформація, має послідовність з трьох мірних векторів спостережень, які в сучасних засобах радіолокаційної розвідки містять не виміряні параметри цілі, а її координати отримані за допомогою перерахунку цих параметрів.

Власне методика фільтрації оцінок елементів вектору стану при умові рівномірного прямолінійного руху цілі може бути представлена наступною сукупністю дій:

1. Визначення екстрапольованого значення (прогнозу) вектору стану з урахуванням його попередньої фільтрованої оцінки і моделі руху цілі.
2. Визначення екстрапольованого значення (прогнозу) вектору спостережень.
3. Розрахунок матриці точності вектору стану, які є показниками якості фільтрації.
4. Оцінка матриці вагових коефіцієнтів з перерахунком невязки до вектору стану.
5. Визначення елементів вектору спостережень та оцінка вектору невязки.
6. Розрахунок квазілінійної фільтрованої оцінки вектору стану.

Для оціни якості даного алгоритму фільтрації оцінок праматерів траєкторії можна розрахувати кореляційну матрицю (2x2) помилок оцінювання координат елементів вектору стану.

Якщо проаналізувати вище вказане, то зрозуміло що елемент кореляційної матриці помилок оцінювання координат елементів вектору стану [1;1] є дисперсією помилки фільтрованої дальності, або першим коефіцієнтом фільтрації. Елемент [2;2] є нічим іншим як дисперсією помилки фільтрованої дальності. А поза діагональні елементи [1;2] і [2;1] характеризують кореляційний зв`язок між оцінками дальності та приростом дальності і є другими коефіцієнтами фільтрації.

Врахування "передісторії" роботи РЛС суттєво покращує показники якості супроводження цілі. При цьому траєкторія, яка сформована на основі оціночних значень, з часом наближається до істинної траєкторії за умов прямолінійного рівномірного руху цілі.

к.т.н. Полуяненко М.О., Онікійчук О.О., Деменко Є.Є., Гончаров М.О., Писаренко Н.В.
(Харківський національний університет імені В. Н. Каразіна)

ОЦІНКА ЙМОВІРНОСТІ ПОДВІЙНИХ ВИТРАТ В БЛОКЧЕЙН СИСТЕМАХ НА ПІДСТАВІ „МОДЕЛІ НЕЗАЛЕЖНИХ ГРАВЦІВ”

Актуальність. В роботі проведено аналіз відомих аналітичних оцінок ймовірності успішної реалізації атаки подвійної витрати на блокчейн системи в основі яких лежать механізми консенсусу на основі доказу виконаної роботи, що використовують геш-функції. Зокрема, розглянуто так звану „Задача про розорення гравця”, показано, що базові припущення про ймовірнісний простір (множину елементарних результатів і ймовірності їх настання) не відповідають реальним процесам, що протікають при встановленні консенсусу на основі доказу виконаної роботи в блокчейн системі. Запропоновано модель «незалежних гравців», яка усуває основні неточності і невідповідності.

Мета. Метою роботи є розвиток та уточнення існуючих методів оцінки ймовірності атаки подвійної витрати на блокчейн системи в основі яких лежать механізми консенсусу на основі доказу виконаної роботи, що використовують геш-функції.

Основна частина. Як правило, всі „класичні” платіжні системи є централізованими, що мають адміністративну ланку, яка забезпечує контроль легітимності будь-якої операції. При цьому, прийняття рішень про легітимність платежу виконує адміністратор, тому платник в змозі лише сформувати заявку на повторну витрату одних і тих же засобів, а адміністратор підтвердить тільки першу заявку, яка надійшла і відкине наступні, що блокує можливість подвійної витрати одних і тих же коштів.

У блокчейн системах передбачається відсутність адміністративного ресурсу, і отже, можливість проведення подвійний витрати одних і тих же коштів стає можливим. Для захисту від атак подвійних витрат продавці можуть приймати різні заходи захисту, найбільш ефективним з них, є очікування включення транзакції з оплатою в один з блоків блокчейн реєстру. При цьому вузол, який формує блок, не допустить включення в блок транзакції, що намагається повторно витратити раніш витрачених коштів. Навіть якщо такий блок буде сформовано вузлом зловмисника, його відкинуть вузли чесної мережі і блок не буде додано до блокчейн реєстр чесних користувачів.

Першим і найбільш вивченим протоколом консенсусу децентралізованих систем є алгоритм „Доказу виконаної роботи”. В його основі лежить вирішення складної обчислювальної задачі. І тільки той, хто першим вирішить цю задачу, отримає право зробити зміну в стан системи. Фактично це означає можливість здійснення транзакції з відчуженням цифрових активів. Таким чином, завдання запобігання подвійного витрати полягає у виключенні (або, принаймні, зниження ймовірності) можливого формування блоку одним і тим же учасником системи. На практиці це досягається залученням величезного числа учасників з відповідним розподілом їх обчислювальних можливостей щодо пошуку прообразів криптографічної функції гешування. Додатково, кожен учасник має можливість передавати права на свої активи тільки після деякого числа сформованих блоків, кратна знижуючи тим самим ймовірність подвійної витрати.

Перші результати по оцінці ймовірності подвійних витрат в децентралізованих системах були опубліковані в работах S. Nakamoto та M. Rosenfeld. Це самі відомі і цитовані роботи даної галузі. Існують також інші публікації, які уточнюють і доповнюють результати приведених авторів. Розрахунки, у згаданих роботах, використовують модель розорення гравця, яка перевіряється методами Монте-Карло. На основі даної моделі отримується формула для розрахунку ймовірності успішного проведення атаки подвійний витрати та надаються рекомендації щодо зведення ймовірності її практичної реалізації до прийнятного мінімуму.

У визначенні завдання про розорення гравця використовується ймовірнісний простір з двома елементарними подіями: „виграв перший гравець”; „виграв другий гравець”. При моделюванні атаки подвійний витрати S. Nakamoto і M. Rosenfeld інтерпретують елементарні результати цього завдання як „блок сформовано чесної мережею” (з ймовірністю такого результату p) і „блок сформований атакуючим” (з ймовірністю q), причому $p=1-q$. Однак, в реальних блокчейн системах ймовірність формування блоку визначається виключно гешрейтом (обчислювальними можливостями) кожного учасника, тобто умова $p=1-q$ не повинна виконуватися.

Наприклад, при гешрейті учасників, що перевищує складність пошуку геш-значення блоку за певний інтервал часу, кожен учасник гарантовано знайде прообраз, тобто сформує блок і, в цьому випадку $p=1$, і $q=1$. У реальних системах складність пошуку прообразу коригується виходячи з обчислювальних можливостей учасників, причому так, щоб блок був знайдений за певний часовий інтервал (наприклад, в криптовалюта біткоіни це 10 хвилин). Якщо припустити, що таке коригування виконується над двома гравцями: „чесна мережа” і „атакуючий”, а p та q – відповідні ймовірності формування блоку за певний часовий інтервал, тоді припущення $p=1-q$ виправдано. Однак в реальній ситуації зловмисник атакує систему не оголошуючи своїх обчислювальних можливостей і, найімовірніше, приховуючи сам факт атаки, тобто припущення $p=1-q$ не має підстав.

Якщо відмовитися від обов’язкового виконання умови $p=1-q$, тоді в результаті кожної спроби (або серії спроб протягом заданого інтервалу часу) простір елементарних події містить такі події:

– елементарна подія „блок сформований чесної мережею та атакуючий не сформував блок” з ймовірністю $p\cdot(1-q)$;

– елементарна подія „блок не сформований чесної мережею та атакуючий сформував блок” з ймовірністю $(1-p)\cdot q$;

– елементарна подія „блок не сформований чесної мережею та атакуючий не сформував блок” з ймовірністю $(1-p)\cdot(1-q)$;

– елементарна подія „блок сформований чесної мережею і атакуючий сформував блок” з ймовірністю $p\cdot q$.

Наведену модель з чотирма елементарними подіями (будемо називати її „модель з незалежними гравцями”) описує реальний імовірнісний процес в блокчейн системах при встановленні консенсусу на основі алгоритму доказу виконаної роботи.

З використанням розглянутих моделей були отримані емпіричні оцінки ймовірності успішного формування ланцюга блоків зловмисником при різних значеннях q та кількості підтверджень, на яку чекає продавець до прийняття факту оплати. Побудовані відповідні функції розподілу ймовірності в залежності від кількості спроб для кожного випробування.

За методами Монте-Карло на основі комп’ютерного моделювання проведено порівняння результатів, отриманих за допомогою обчислювального моделювання атаки подвійний витрати на основі моделі розорення гравця і моделі незалежних гравців. Порівняння проведено для різних можливостей зловмисника (ймовірності сформувати блок), різної кількості сформованих блоків після яких угода вважається підтвердженою, різної тривалості гонки (кількості блоків протягом яких зловмисник продовжує спроби наздогнати чесну мережу).

Висновок. Отримано значну відмінність результатів (відносна помилка моделей досягає 99 %), одержаних при обчислювальному моделюванні з використанням моделі незалежних гравців від моделі розорення гравця. На основі отриманих результатів можна стверджувати про помилковість використання моделі розорення гравця для оцінки ймовірності успішної атаки подвійний витрати на протокол консенсусу на основі доказів виконаної роботи.

д.т.н. Почерняєв В.М. (ОНАЗ)
Помін А.Г. (ВІТІ)
Колодійчук Л.В. (ВІТІ)

РАДІОРЕЛЕЙНА КОМПОНЕНТА МОБІЛЬНОЇ ЦИФРОВОЇ ТРОПОСФЕРНО-РАДІОРЕЛЕЙНОЇ СТАНЦІЇ

У районах стихійних лих і техногенних катастроф, при виникненні надзвичайних і позаштатних ситуацій можливість управління обстановкою, що склалася, у вирішальній мірі визначається наявністю постійно діючого зв'язку, стійкого до зовнішніх впливів. В таких умовах радіозв'язок є основним видом зв'язку при організації управління в даній ситуації, як правило, вузли фіксованого зв'язку виявляються віддаленими від розгорнутих центрів управління. Залежно від ситуацій, що виникають зв'язок забезпечується на основі використання радіосистем НВЧ діапазону: радіорелейних, супутникових або тропосферних. Залежно від масштабів лиха виникає задача встановлення зв'язку через складно доступні для прокладки кабелю або побудови антенних щогл місцевості. У зоні проведення антитерористичних операцій виникають завдання організації стійкого зв'язку через територію, яка не контролюється власними військовими формуваннями. З наземних типів зв'язку можливим рішенням може бути розгортання загоризонтних ліній зв'язку, що складаються з цифрових тропосферних станцій. Однак не варто виключати і варіант, коли одна сторона лінії зв'язку або обидві сторони повинні бути прив'язані до стаціонарних вузлів операторів зв'язку. Таку прив'язку в польових умовах здійснюють засобами радіорелейного зв'язку прямої видимості.

Таким чином, з метою організації стійкого зв'язку при зазначених вище ситуаціях можуть використовуватися як мобільні станції радіорелейного, так і тропосферного типу, які в англомовній літературі відносяться до засобів зв'язку типу Line-Of-Sight (LOS) і Beyond Line-Of-Sight (BLOS) відповідно. Світові виробники наземного радіо обладнання НВЧ діапазону мають в своєму арсеналі сучасні рішення систем як типу LOS, так і типу BLOS. Однак комбінованих варіантів, які пропонували б на єдиній мобільній транспортній базі реалізацію і одного і іншого рішення (LOS + BLOS), вочевидь, не існує. Тут слід виділити оригінальне рішення корпорації Raytheon (США), яка створила мобільну цифрову станцію зв'язку DART-T (BLOS + SATCOM). При зміні оперативної або надзвичайної ситуації виникає необхідність перейти з одного типу радіозв'язку на інший і рішення LOS + BLOS в такій ситуації може опинитися єдино можливим.

Тому, створення комбінованої станції – мобільної цифрової тропосферно-радіорелейної станції (МЦТрРРС) – на єдиній транспортній платформі цілком виправдано. Особливістю МЦТрРРС як складної радіотехнічної системи є єдина система управління та частотоформування для тропосферної та радіорелейної компонент.

З огляду на науково-технічний потенціал України, що залишився, виробництво таких станцій може бути освоєно вітчизняною промисловістю при тому в декількох конструктивних варіантах. Для даної МЦТрРРС будемо користуватися термінологією тропосферної та радіорелейної компонент (ТК та РРК).

Метою роботи є дослідження можливості побудови радіорелейної компоненти МЦТрРРС на основі існуючої мобільної цифрової радіорелейної станції „Дебютант". В роботах [1 – 3] надані обґрунтовані напрямки перспектив розвитку мобільних цифрових радіорелейних та тропосферних станцій. При створенні станції враховувалася специфіка функціонування лінії загоризонтного зв'язку. В основі побудови ліній загоризонтного зв'язку лежать два механізми поширення радіохвиль:

– на інтервалах 50-80 км – дифракційне поширення радіохвиль;

– на інтервалах більше 80 км – розсіювання радіохвиль на неоднорідностях тропосфери.

Особливістю ліній загоризонтного зв'язку є те, що на них застосовується рознесений прийом сигналів. У даній станції застосовується просторово рознесений прийом. Станція також має систему адаптації по частоті і систему адаптації по потужності.

Система адаптації по частоті передбачає вибір оптимальної частоти. В основі такого способу є постійний аналіз частот на прийомі, що входять в робочу смугу і визначення найбільш оптимальної з них. Ця частота має максимальний коефіцієнт передачі тропосферного сигналу і передавач протягом короткого тимчасового інтервалу перебудовується на неї.

Система адаптації по потужності передбачає автоматичне регулювання потужності передавача. На приймальній стороні вимірюється відношення сигнал/(шум + завада) і достовірність інформації, що приймається. Оскільки, різниця в медіанних коливаннях рівня сигналу через метеоумови місяця (року) становить 10 ... 15 дБ, а протягом доби медіанний рівень сигналу змінюється в межах до 4 дБ взимку і до 10 дБ влітку, то діапазон зміни потужності передавача повинен становити 20 … 25 дБ.

У МЦТрРРС, як в тропосферних, так і в радіорелейних режимах використовується дуплексний метод передачі/прийому. Обмін інформацією між двома кореспондентами здійснюється одночасно в двох частотних діапазонах для прийому і передачі окремо.

Управління МЦТрРРС здійснюється з єдиного для тропосферного та радіорелейного режимів роботи об'єкта управління (виносного або стаціонарного пульта управління). Слід зауважити, що передавальний НВЧ тракт і збудник-гетеродин також є загальними для тропосферної та радіорелейної компонент МЦТрРРС.

Структурна схема приймально-передавальної частини МЦТрРРС показана в роботі [4, рис.1]. Проте схема радіорелейної компоненти повністю не розкрита.

МЦТрРРС є перспективною радіотехнічною системою не тільки для Збройних Сил України, а й і для Департаменту з надзвичайних ситуацій, Державній прикордонній службі, Держспецзв'язку та комерційним структурам, що потребують мобільних засобів зв'язку. Доцільно прийняти рішення щодо побудови радіорелейної компоненти МЦТрРРС на базі існуючої станції „Дебютант". Це пов'язано з тим, що станції „Дебютант" виробляються підприємством України в рамках Державного оборонного замовлення.

ЛІТЕРАТУРА

1. Почерняев В.Н. Состояние и направления развития мобильных цифровых радиорелейных систем / В.Н. Почерняев, В.С. Повхлеб // Системи озброєння і військова техніка – 2018. – № 1. – С. 183 – 188.

2. Почерняев В.Н. Состояние и направления развития мобильных цифровых тропосферных систем связи / В.Н. Почерняев, В.С. Повхлеб // Системи озброєння і військова техніка – 2018. – № 2. – С. 51 – 60.

3. Пат. 112217 Україна, С2. Мобільна цифрова тропосферно-радіорелейна станція / В.М. Почерняєв, В.С. Повхліб; заявник і патентовласник Почерняєв В.М., Повхліб В.С.; заявл. 12.09.2014; опублік. 10.08.2016, Бюл. № 15. – 8 с.

4. Почерняев В.Н. Мобильная цифровая станция СВЧ диапазона двойного назначения / В.Н. Почерняев, В.С. Повхлеб // Наукові праці ОНАЗ ім. О.С.Попова – 2014. – №2 – С. 76 – 82.

д.т.н. Пушкарьов Ю. О. (ЖВІ)
к.т.н. Ревенко В.Б. (ЖВІ)

МЕТОД СИНТЕЗУ СЛІДКУВАЛЬНИХ АВТОМАТИЧНИХ СИСТЕМ УПРАВЛІННЯ ПІДВИЩЕНОЇ ТОЧНОСТІ

Актуальність, постановка задачі.

Однією з основних задач теорії автоматичного управління (ТАУ) є задача синтезу систем, у результаті вирішення якої визначається склад, структура системи автоматичного управління (САУ) та параметри всіх її пристроїв із умов : задоволення заданому комплексу технічних умов забезпечення стійкості та якості перехідних процесів (підвищення швидкодії, зменшення перерегулювання та ін.) , підвищення точності управління в сталому режимі.

Як визначено в ТАУ, методи синтезу САУ із умов заданих показників якості – це є методи розв'язання задачі синтезу регуляторів (коректуючих пристроїв), які точно визначають їх структуру та параметри.

Для комбінованих САУ, а також САУ, які еквівалентні комбінованим автоматичним системам існують відомі методи синтезу регуляторів за умови компенсації зовнішніх збурень та відтворення задавальних впливів із умов досягнення інваріантності помилки щодо даних впливів.

При побудові систем , які еквівалентні комбінованим, як правило , використовувалася вихідна управляєма величина (вихід системи).

Це вимогало додаткових апаратурних витрат та вносило додаткові помилки вимірювань управляючої величини.

Мета. Підвищення точності слідкування та оцінювання за динамічними об'єктами в умовах апріорної невизначеності їх руху і наявності збурень.

Основні положення.

Запропоновано метод двоконтурних систем, що еквівалентні комбінованим.

Проведено роздільний синтез оптимального фільтра оцінювання вхідної корисної дії та синтез регулятора для управління об'єктом управління слідкувальної системи із застосуванням методу двоконтурних систем, що еквівалентні комбінованим в умовах не вимірюваної вхідної дії та наявності адитивних збурень.

Результати моделювання слідкувальних систем з фільтрами (регуляторами) управління та фільтрами компенсації випадкових збурень показали їх значну ефективність.

Напрямками практичного використання запропонованого методу є радіотехнічні слідкувальні системи за кутовими координатами, системи термінального управління , де інваріантность (нульова помилка управління) повинна бути досягнута не в теперішній час,а в кінцевий момент часу та ін..

Висновок. Розглянуто питання синтезу САУ , що еквівалентні комбінованим , в умовах наявності одночасно , як вхідної (задаючої) дії, так і зовнішніх збурень та завад. Запропоновано метод синтезу слідкувальних автоматичних систем управління підвищеної точності.

Запропонований метод доцільно застосовувати при побудові слідкувальних систем озброєння , військової техніки, (особливо радіотехнічних та телекомунікаційних, де вхідна корисна дія не вимірюється і комбіноване управління неможливе).

к.т.н. Рибка С.В. (ІПМЕ НАНУ)
к.т.н. Корольов А.П. (ВІТІ)
к.т.н. Варава І.А. (НТУУ „КПІ”)

ПРОГРАМНИЙ ЗАСІБ ПРОЕКТУВАННЯ ЦИФРОВИХ ФІЛЬТРІВ МЕТОДОМ ЧАСТОТНОЇ ВИБІРКИ

Існує багато програмних засобів для проектування цифрових фільтрів. Наприклад у пакеті прикладних MATLAB є можливості моделювання та розрахунку різних типів фільтрів. Проте фільтрам на основі частотної вибірки приділяється мало уваги і загально-відомих та доступних програмних засобів їх розрахунку немає. Такі фільтри мають високу обчислювальну ефективність і гнучкість при переналаштуванні смуг частот, що аналізуються. Вони можуть бути корисними при проектуванні цифрових пристроїв спектрального аналізу, обробці мовних сигналів, квадратурній фазовій маніпуляції сигналів, систем управління зброєю.

Пропонується розроблений програмний засіб, за допомогою якого можна провести інтерактивне проектування цифрових фільтрів методом частотної вибірки на основі модифікованої передавальної функції з дійсними коефіцієнтами. Інтерфейс користувача може бути відображений українською та англійською мовами. Користувачі спершу переходять за посиланням на головну сторінку публічної частини сайту, де приводиться основна інформація про можливості програмного продукту.

Меню містить посилання для переходу на сторінки «Головна», «Дизайнер фільтрів», „Публікації” та „Контакти”. Основна робота здійснюється на сторінці «Дизайнер фільтрів»

Користувачу надається форма для вводу основних вимог до параметрів цифрового фільтру, що проектується:

- частоти зрізу;
- задане гарантоване загасання у смузі затримування;
- задана нерівномірність загасання у смузі пропускання.

При введенні цих параметрів автоматично розраховуються параметри, які застосовуються при апроксимації передавальної функції: порядок фільтру, значення частот у вузлах інтерполяції, частотні коефіцієнти, початкові інтерпольовані значення вагових коефіцієнтів у смузі пропускання та транзитній смузі, а також інші коефіцієнти. Одночасно відбувається оновлення графіку частотної характеристики загасання.

У алгоритмі апроксимації застосовуються:

– спосіб найкращого розташування сплесків загасання в смузі затримування фільтру на основі частотної вибірки;

– критерій досягнення глобально-оптимального рішення задачі апроксимації в смузі затримування фільтру на основі частотної вибірки;

– спосіб досягнення заданої величини нерівномірності характеристики загасання в смузі пропускання за допомогою коефіцієнтів Гіббса;

– властивість симетрії частотних характеристик передавальної функції;

– спосіб зменшення ширини транзитної смуги;

– властивість ідентичності вагових коефіцієнтів передавальної функції.

Рішення може бути використане для проектування цифрових гребінок смугових фільтрів і застосоване при обробці широкосмугових сигналів в радіолокації, гідролокації, телекомунікаціях, медицині. Виконується робота зі створення веб-сайту проектування цифрових фільтрів методом частотної вибірки. Адміністративна частина сайту дозволяє переглядати статистику відвідувань та повідомлення залишені за допомогою форми зворотного зв’язку із сторінки „Контакти”.

Веб-ресурс реалізовано за допомогою стеку технологій HTML5, JavaScript, PHP та MySQL.

к.т.н. Рижов Є.В. (НАСВ)
к.т.н. Сакович Л.М. (ІСЗЗІ НТУУ „КПІ”)

МЕТОД РОЗПОДІЛУ ЧАСУ ПРИ ВІДНОВЛЕННІ РАДІОЕЛЕКТРОННИХ ЗАСОБІВ З КРАТНИМИ ДЕФЕКТАМИ

При отриманні радіоелектронними засобами в польових умовах аварійних або бойових ушкоджень у них виникають кратні (множинні) дефекти. Тоді відновлення працездатності проводиться поетапно:

– спочатку на місці пошкодження екіпажами виконується попередня дефектація з метою встановлення ступеня пошкодження;

– на другому етапі силами фахівців ремонтного органу проводиться повна дефектація з усуненням явних дефектів;

– на третьому етапі з використанням засобів вимірювальної техніки і діагностичних програм усуваються приховані дефекти і відновлюється працездатність виробів.

Питання вдосконалення системи ремонту радіоелектронних засобів, особливо при їх поточному ремонті, досить широко використані в роботах провідних фахівців. Вони розглядають методи і способи відновлення радіоелектронних засобів, оцінки їх реального технічного стану, розробки ефективного діагностичного забезпечення поточного ремонту. Особливості відновлення радіоелектронних засобів з кратними дефектами вивчені в недостатній мірі, що не сприяє ефективній роботі ремонтних органів при усуненні аварійних і бойових ушкоджень, особливо в польових умовах.

У відомих джерелах використовуються напрямки підвищення ефективності поточного ремонту радіоелектронних засобів при наявності в них тільки одного дефекту. Однак при відновленні радіоелектронних засобів з кратними дефектами в умовах віддалення від баз ремонту і постачання потрібно мінімізація середнього часу відновлення за рахунок підвищення ефективності дефектації та діагностування. Тому використання і доведення до практичної реалізації питань визначення реального технічного стану радіоелектронних засобів при наявності кратних дефектів досить актуальне наукове завдання.

Метою доповіді є формалізація процесу розподілу часу для його мінімізації по етапах відновлення радіоелектронних засобів з кратними дефектами при обліку якості метрологічного та діагностичного забезпечення.

Запропонований метод дозволяє мінімізувати середній час відновлення при усуненні кратних дефектів, отриманих в результаті аварійних або бойових ушкоджень. Він полягає в комплексному розгляді складових процесу ремонту після попередньої дефектації на місці пошкодження і оцінки прогнозованої кратності дефектів.

Розроблено блок-схема алгоритму вирішення зазначеного завдання, що відрізняється від відомих урахуванням ймовірності правильної постановки діагнозу та метрологічної надійності засобів вимірюваної техніки, яка використовується.

Застосування методу в конкретних умовах дозволяє кількісно оцінити час реалізації кожного етапу відновлення і обґрунтовано рекомендувати перерозподіл зусиль для мінімізації середнього часу відновлення працездатності радіоелектронних засобів з кратними дефектами.

Наведено приклад реалізації методу, де досліджено вплив керованих змінних на його ефективність. Використання отриманих результатів дозволяє підвищити пропускну здатність військових ремонтних органів при відновленні техніки із слабкими і середніми бойовими ушкодженнями, як в польових умовах, так і на пунктах технічного обслуговування і ремонту.

Запропонований метод доцільно реалізувати в програмному забезпеченні перспективних апаратних технічного забезпечення модульного типу.

к.т.н. Рихальський О.Р. (ЖВІ)
Натальчук С.В. (ЖВІ)

ОЦІНКА ВПЛИВУ ПАРАМЕТРІВ КАНАЛУ ЗВ'ЯЗКУ НА ЯКІСТЬ ПЕРЕДАЧІ ІНФОРМАЦІЇ В РУХОМИХ СИСТЕМАХ СТАНДАРТУ GSM

В умовах ведення гібридних війн важливе місце в інформаційному протиборстві займає мобільний зв'язок.

Робота мобільного зв'язку забезпечується розвинутою мережею базових станцій, які передають інформацію на комутаційні центри за допомогою радіочастотних сигналів.

Для підвищення якості мобільного зв'язку оператори збільшують кількість базових станцій та здійснюють їх постійне переоснащення відповідно до найновітніших технологічних розробок галузі.

З цією метою розробляється частотно-територіальний план (ЧТП).

Під час проектування системи виконується прив'язка системи вибраного стандарту до реальної території.

Для цього необхідно: визначити допустиму кількість мовних каналів у стільнику; забезпечити трафік відповідно до демографічної ситуації на території; встановити кількість стільників і їх межі; розрахувати потужність передавача базової станції (БС) тощо.

Аналіз стану проблеми частотно-територіального планування мережі рухомого і фіксованого радіозв'язку показує, що для її вирішення не існує строго формалізованих алгоритмів, а вхідні дані часто виявляються недостатніми і неточними, це дозволяє зробити висновок про те, що найбільш конструктивним підходом до вирішення даного складного завдання є декомпозиція всієї процедури планування на ряд етапів.

Крім того, дану проблему можна вирішити за рахунок оптимізації місць розташування БС, потужності передавачів, висот антен та їх типів (ненаправлені або з направленням за секторами) і розподілу частот між БС.

При розробці методики покращення якості зв'язку дуже важливо врахувати умови поширення радіохвиль.

Для організації мережі стільникового зв'язку, а саме визначення оптимального місця розташування і кількості БС, а також для вирішення інших завдань необхідно вміти розрахувати характеристики сигналу в будь-якій точці простору в межах всієї зони обслуговування.

Міське середовище утворює специфічні умови для поширення радіохвиль.

Тіньові зони, багаторазове відбиття і розсіювання хвиль формують багатопроменеві поля зі складною інтерференційною структурою і різкими просторовими змінами рівня сигналу.

Багатопроменевий характер поширення радіохвиль, коли в точку прийому надходять хвилі з різних напрямків і з різними часовими затримками, породжує явище міжсимвольної інтерференції в разі передачі кодових послідовностей.

Спотворення сигналу, обумовлені міжсимвольною інтерференцією, можуть викликати серйозні погіршення характеристик системи та якості високошвидкісної передачі цифрової інформації, якщо тривалість затримки перевищує тривалість символу.

В доповіді представлені результати аналізу побудови та функціонування мобільної системи зв'язку цифрового стандарту GSM, наведена методика оцінки показників якості каналу зв'язку (рівень перешкод за сусідніми частотними каналами та ймовірність помилки на один біт), які враховують побічні випромінювання в цій мобільній системі.

Показано можливість підвищення співвідношення сигнал/перешкода за рахунок застосування секторних антен.

д.т.н. Романенко І. О. (ЦНДІ ОВТ ЗС України)

АНАЛІЗ ЗАВДАНЬ І МЕТОДІВ ОЦІНКИ ТА ВИБОРУ АЛЬТЕРНАТИВ РІШЕНЬ

Процес прийняття рішень складається з ряду стадій (етапів). На початковому етапі необхідно виявити проблему, проблемну ситуацію або певну предметну область, в яких потрібне прийняття рішень.

Термін „рішення” має багато смислових значень. Це можуть бути дії щодо вирішення проблем, що призводять до якогось результату, наслідки яких необхідно оцінити. Під рішенням розуміють також деякі об’єкти, системи, що вимагають оцінювання. Рішення це також різні варіанти, альтернативи, можливості щодо дій і об'єктів.

На наступному етапі необхідно змістовно описати предметну область, виявити цілі прийняття рішень і обмеження.

Далі потрібно здійснити збір та аналіз детальної інформації про предметну область. У ряді випадків необхідно побудувати модель, визначити область альтернатив (варіантів) рішень, виконати генерацію рішень, сформулювати завдання прийняття рішень.

На наступному етапі здійснюється прийняття рішень на основі обраних (розроблених) методів. Виконується оцінка варіантів рішення, їх порівняння, класифікація, ранжування, вибір найкращого.

І, нарешті, заключна фаза пов'язана з реалізацією рішення і оцінки його наслідків.

Залежно від повноти і вихідних даних завдання вибору рішень можуть бути добре структурованими, слабо структурованими і неструктурованими. Для добре структурованих задач дані формулюються в кількісному вигляді, для слабо структурованих задач вони містять кількісні опису з домінуванням якісних і невизначених факторів, для неструктурованих завдань дані представляються у вигляді якісного опису вихідних факторів і взаємозалежностей між ними.

Вибір рішень може здійснюватися в умовах визначеності, ризику або невизначеності. В умовах визначеності відомі вихідні дані і наслідки кожної альтернативи рішень.

Умови ризику мають місце, якщо відомі ймовірності альтернатив рішень або відомий закон розподілу їх ймовірностей. Тоді задача зводиться до вибору статистичних рішень. У свою чергу, умови ризику можна визначити як умови стохастичною невизначеності, породжені випадковими факторами, які при їх масовій появі мають властивість статистичної стійкості і описуються будь-яким законом розподілу ймовірності.

Умови невизначеності, при яких закон розподілу ймовірностей для невизначених факторів невідомий, визначаються як умови статистичної невизначеності. Умови статистичної невизначеності, в свою чергу, діляться на два види: по-перше, з відомими параметрами розподілу (математичне очікування, дисперсія та інші характеристики випадкової величини); по-друге, з невідомими параметрами розподілу.

До основних завдань оцінки і вибору альтернатив рішень можна віднести такі:

оцінка альтернатив рішень;

порівняльна оцінка і ранжування безлічі альтернатив рішень;

визначення стратегій оцінювання альтернатив рішень;

визначення значень часткових показників рішень по заданих значенням узагальненого показника;

пошук значень часткових показників, що забезпечують необхідні значення узагальненого показника;

пошук найкращих рішень (значень часткових показників), що забезпечують необхідні значення узагальненого показника.

Можна виділити одно- і багатокритеріальні методи оцінки і вибору альтернатив рішень.

В однокритеріальному випадку вважаються відомими:

безліч альтернатив рішень (об'єктів, варіантів дій);

оцінка альтернатив за обраним критерієм (показником) та правило вибору найкращого варіанту.

Іншим випадком завдання вибору є ранжування варіантів рішень відповідно до безлічі оцінок альтернатив. Найбільш значним для практичного використання є випадок оцінки і вибору альтернатив за багатьма критеріями.

У багатокритеріальному випадку кожному варіанту можна поставити в відповідність вектор, що представляє оцінки варіанту за критеріями (показниками).

Далі підходи до порівняння і вибору варіантів рішень можуть бути розділені на дві великі групи: зведення і не зведення багатьох критеріїв до одного.

Методи, засновані на незведенні багатокритеріальних задач оцінки і вибору варіантів рішень до одного критерію, ставлять своїм завданням порівняння варіантів на основі векторів оцінки за всіма критеріями.

Серед важливих факторів, що враховуються при вирішенні цього завдання, можна вказати вагу (важливість) критеріїв. Часто ці методи використовуються в іншій постановці: пошук оптимальних рішень на безлічі параметрів, що визначають умови прийняття рішень.

Серед методів цієї групи можна виділити:

метод домінування;

метод на основі глобальних критеріїв;

лексикографічне упорядкування;

методи математичного програмування;

методи порогів;

методи теорії мультимножин та інші.

Застосування цих методів обумовлено, як правило, незалежністю критеріїв, їх повною визначеністю.

У разі використання методів, заснованих на зведенні багатокритеріальних завдань оцінки і вибору варіантів рішень до одного критерію, завдання вибору вирішується на основі побудови інтегрального (узагальненого) критерію.

Для цього використовуються різноманітні способи агрегування, „згортки” показників, тобто побудови різних узагальнюючих показників, перш за все, адитивних і мультиплікативних.

Адитивний узагальнюючий критерій (показник) виходить як зважена сума оцінок за частковими критеріями (показниками).

Однак наведені методи не завжди адекватно відображають особливості завдань оцінки і вибору, зокрема, взаємозалежність, суперечливості окремих показників.

Підхід, заснований на згортці багатьох критеріїв в один, використовується у багатьох методах теорії прийняття рішень, серед яких можна виділити наступні:

методи, засновані на теорії цінності, корисності;

методи аналізу ієрархій;

методи нелінійної згортки;

методи теорії нечітких множин та інші.

Підхід до багатокритеріальної оцінювання складних об’єктів, заснований на зведенні багатьох критеріїв до одного, привабливий тим, що він знижує трудомісткість таких процедур теорії прийняття рішень, як порівняння, ранжування, класифікація і вибір варіантів (альтернатив).

Аналіз існуючих методів дозволяє зробити висновок про те, що вони не в повній мірі відображають особливості предметної області, які полягають в невизначеності, розвиненої системи сильно взаємодіючих різноякісних показників, складності оцінюваних об'єктів.

Загальним обмеженням використання розглянутих методів багатокритеріального оцінювання альтернатив є складність формування багаторівневої структури оцінювання, а також вибору і налаштування операцій згортки показників.

д.т.н. Романюк В.А. (ВІТІ)

АЛГОРИТМ ПОЗИЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ АЕРОПЛАТФОРМ ДЛЯ ЗБІЛЬШЕННЯ ПРОПУСКНОЙ ЗДАТНОСТІ ПОВІТРЯНОЇ МЕРЕЖІ

Одним із завдань управління наземно-повітряною радіомережею (НПР) є оптимізація пропускної здатності повітряної мережі (ПМ). Відомо, що швидкість передачі даних у сучасних широкосмугових радіоканалах, крім інших факторів, суттєво залежить від відстані між вузлами. Крім цього, гранична пропускна здатність телекомунікаційної аероплатформи (ТА) обмежена протоколом канального рівня [1]. Тому виникає завдання для системи управління повітряною мережею – знайти положення ТА в зоні обслуговування своїх наземних вузлів, яке забезпечить максимум (заданий рівень) пропускної здатності ПМ при використанні певного протоколу канального рівня [2].

Задано: $k = 1 \ldots K$ – множина задіяних ТА, їх початкове положення у просторі, відповідно, множина зон покриття наземних вузлів;

R_u – радіус покриття u-ї ТА; n_u – множина наземних вузлів (НВ), які покриті u-ою ТА;

матриця вхідного навантаження $\boldsymbol{G} = \|g_{ab}\|$ за напрямами a-b, $a,b \in K$, a – ТА-відправник, b – ТА-отримувач;

маршрути передачі за напрямами передачі a-b – $M = \{m_{ab}\}$;

план розподілу навантаження по радіоканалам згідно визначених маршрутів $\boldsymbol{G} = \|g_{uw}\|$, де $a, b, u, w \in K$;

існуючі відстані між ТА $\boldsymbol{R} = \|r_{uw}\|$, $r_{uw} \le r_{\max}$, які визначають потенційну швидкість передачі (пропускну здатність) між сусідніми ТА s_{uw}, $u,w \in K$; $r_{\max}$ – гранична дальність радіозв'язку між ТА, яка може бути розрахована, виходячи з параметрів радіозасобів та відношення сигнал-шум в точці прийому при певній швидкості передачі [2];

значення швидкостей передачі між ТА для набору сигнально-кодових конструкцій, ширини смуги пропускання відповідного протоколу доступу до радіоканалу;

потужності передачі ТА – P_w.

Обмеження та припущення: кожна ТА здійснює інформаційний обмін із сусідніми ТА без інтерференції. Це припущення може бути досягнуто наступними шляхами: кожна ТА обладнана кількома прийомопередавачами (інтерфейсами); кожна ТА реалізує технологію MU-MIMO (Multi-User Multiple-Input-Multiple-Output).

Всі ТА мають однакову максимальну дальність передачі, яка значно більша дальності передачі між ТА-наземний вузол. Реалізовано частотно-територіальне планування зон обслуговування наземних вузлів. Значення сигнал/шум SNR постійно вимірюється в ТА з метою динамічного призначення сигнально-кодової конструкції для кожного фрейму даних, який передається.

Необхідно: знайти положення ТА, які максимізують пропускну здатність повітряної мережі (окремого напряму передачі) при визначених навантаженні та маршрутах передачі, або задовольнити задане навантаження в повітряній мережі (за напрямом передачі).

Рішення. Пропускна здатність мережі ТА S визначається сумою пропускних здатностей s_{ab} в напрямах передачі a-b, пропускна здатність напряму дорівнює сумі пропускних здатностей l-маршрутів передачі, пропускна здатність маршруту s_{mab} дорівнює мінімальному значенню пропускних спроможностей радіоканалів, які входять до його складу:

$$S = \sum_{i=1}^{n} s_{ab},\ s_{ab} = \sum_{l=1}^{L} m_l,\ s_{m_{ab}} = \min\{s_{uw}\},\ uw \in m_{ab},\ a,b,u,w \in K, \qquad (1)$$

де m_{ab} – маршрут від ТА-відправника a до ТА-отримувача b, s_{uw} – пропускна здатність між сусідніми ТА u та w.

Цільова функція визначається як максимум (забезпечення заданої) пропускної здатності всіх напрямів передачі (2, 3):

$$\max S\ (S \geq S_{зад}), \quad (2)$$

або максимум (забезпечення заданої) пропускної здатності в визначених напрямах передачі *a*-*b*:

$$\max s_{ab}\ (s_{ab} \geq g_{ab}), \quad (3)$$

при обмеженнях (4 – 7)

на відстань можливого переміщення *u*-го ТА – $0 \leq d_u \leq d_{u\max}$, (4)

на значення пропускної здатності радіоканалів між ТА – $s_{uw} \geq g_{uw}$, (5)

на рівень вхідного навантаження *i*-х наземних вузлів на кожну ТА в своїй зоні обслуговування

$$\Theta_u - \ g_u(\Theta_u) = \sum_{i \in 1}^{n_u} g_i \leq s_{u\max}, \forall i \in \Theta_u, \quad (6)$$

на кількість покритих наземних вузлів *u*-ою ТА – $n_u \leq n_{u\min}$. (7)

Основні етапи алгоритму збільшення пропускної здатності в повітряній мережі шляхом зміни положення ТА полягають в наступних кроках:

1. Визначити нове положення кожної ТА у просторі (при забезпеченні заданого рівня покриття визначених наземних вузлів (7), яке призводить до зменшення відстані із сусідніми ТА і збільшення пропускної здатності радіоканалів між ними.

2. Визначити нові пропускні здатності маршрутів відповідно нових отриманих значень пропускних спроможностей радіоканалів між ТА.

3. Перерозподілити вхідний трафік згідно нових значень пропускних здатностей маршрутів для задоволення заданого рівня вхідного трафіка.

Якщо вимоги передачі трафіка задоволені, то закінчити алгоритм, інакше перехід до кроку 1.

На рис. 1 продемонстрований варіант зміни положення чотирьох ТА для забезпечення заданих чотирьох напрямів передачі з навантаженням g_{13}=3, g_{14}=3, g_{34}=6, g_{24}=4 за визначеними маршрутами передачі m_{13}={1-2-3}, m_{14}={1-2-4}, m_{34}={3-2-4}, m_{24}={2-4}. На вихідному положенні ТА при сумарному навантаженні $G = 16$ вихідна сумарна пропускна здатність мережі дорівнює сумі пропускних спроможностей напрямів (вираз 1): $S = s_{13} + s_{14} + s_{34} + + s_{24} = 3 + 3 + 3 + 3 = 12$ (рис. 1а).

Після прийняття рішення з переміщення ТА відбулись зміни пропускних здатностей радіоканалів між ТА: $s_{12} = 8 \rightarrow s_{12} = 7$, $s_{23} = 6 \rightarrow s_{12} = 10$, $s_{24} = 9 \rightarrow s_{24} = 12$. При аналогічному вхідному навантаженні $G = 16$ пропускна спроможність мережі вже дорівнює $S = 3+3+6+4 = 16$ (рис. 1б) та задовольняє вимогам навантаження.

Основна проблема – це значна кількість варіантів розміщення ТА. Тому необхідно обмежити кількість можливих місць розміщення ТА для підвищення пропускної здатності радіоканалів між ТА.

Потенційна можливість зміни відстані між ТА d_{uw} залежить від граничного значення можливого переміщення ТА $d_{uw\max}$, яке, відповідно, залежить від параметрів радіообладнання наземних вузлів (потужність передавача, коефіцієнти підсилення антени тощо), цільової функції управління (наприклад, відсоток покриття наземних вузлів).

Наприклад, якщо наземні вузли не мають режиму маршрутизації за протоколами MANET, тоді ТА повинні покривати всі наземні вузли, або цільова функція управління НПР визначає необхідність покриття всіх наземних вузлів ТА (рис. 2а).

Якщо наземні вузли мають режим MANET та можуть здійснювати обмін між собою, тоді цільовою функцію може бути забезпечення зв'язності окремих підмереж наземних вузлів. Крім цього, це дає можливість значно збільшувати розмір кола можливого переміщення ТА (рис. 2б).

Цільова функція (ЦФ) в формулах (2, 3) є невипуклою і тому може мати локальні максимуми. Відомі методи отримання рішення таких рівнянь мають значну обчислювальну складність. Тому пропонується використати ітераційний алгоритм для обчислення наближеного значення положення ТА, яке намагається максимізувати пропускну здатність

між ТА. Цей алгоритм оцінює пропускну здатність в різних положеннях ТА в середині кола переміщення і вибирає позицію, яка має максимум розрахованої пропускної здатності.

Враховуючи, що практично неможливо розрахувати пропускну здатність у кожній точці всередині кола переміщення ТА, яке містить безліч точок, визначається сітка точок всередині кола, як показано на рис. 3. Для досягнення заданої точності обчислень крок сітки можна регулювати відносно значення, яке залежить від кроку зміни швидкості передачі від відстані за обраним МАС-протоколом.

Алгоритм пошуку рішення системою управління НПР включає наступні кроки:

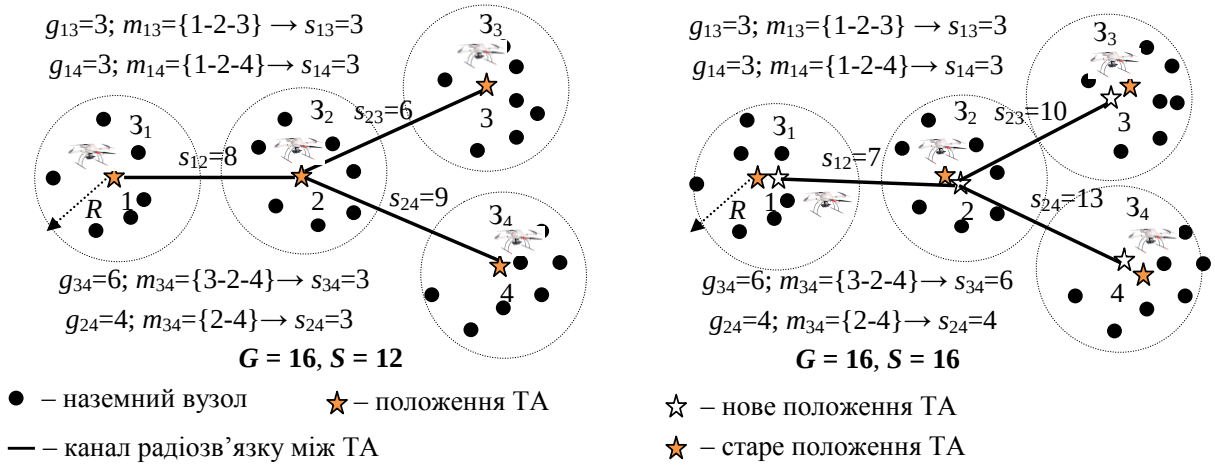
1. Збір даних про стан повітряної мережі (координати розміщення, потужність передачі, співвідношення сигнал/шум, значення пропускної здатності радіоканалів тощо).

2. Аналіз виконання вимог інформаційного обміну.

Перевірка наявної пропускної здатності напрямів (маршрутів, радіоканалів) передачі визначеному рівню вхідного навантаження (обмеження 3).

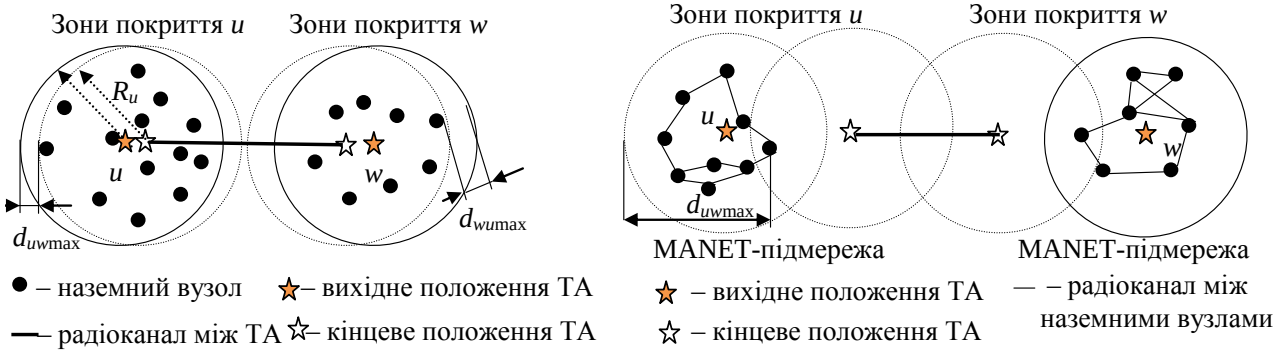
3. Визначення пріоритету цільових функцій (ЦФ) управління мережею.

4. Розрахунок для кожної *u*-ої ТА значення відстані максимально можливого переміщення $d_{uw\max}$ між всіма сусідніми *w*-ми ТА.



а) вихідне положення ТА б) кінцеве рішення з положення ТА

Рис. 1. Рішення про зміну положення ТА для збільшення пропускної здатності ПМ



а) наземні вузли без режиму MANET б) наземні вузли з режимом MANET

Рис. 2. Ілюстрація відстані можливого переміщення ТА

ЯКЩО ЦФ – збереження всіх наземних вузлів зон обслуговування ТА, ТО – побудова кола можливого переміщення кожного ТА.

ЯКЩО ЦФ – максимізація пропускної здатності в зоні обслуговування ТА, ТО – пошук рішення з переміщення для цієї ЦФ [4];

ЯКЩО ЦФ – максимізація пропускної здатності в повітряній мережі,

ТО – пошук рішення з переміщення кожного ТА за межами кола обслуговування (з обмеженням на довжину маршрутів наземних вузлів, які опиняться за межами зон обслуговування ТА).

.

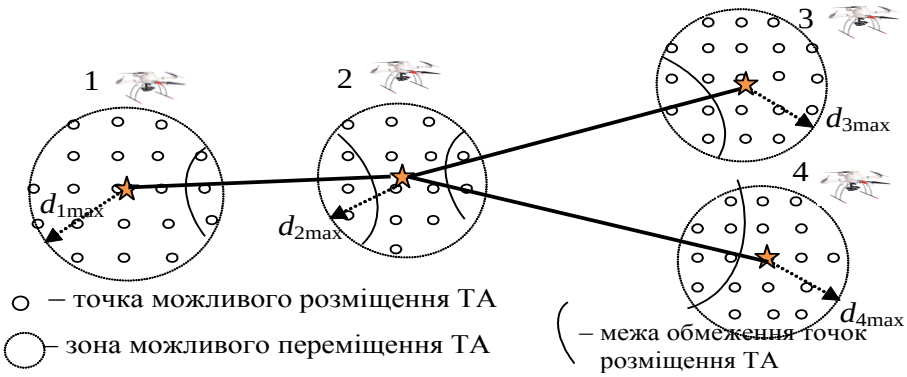


Рис. 3. Можливі місця розміщення ТА в зоні переміщення

5. Для кожної *u*-ої ТА розрахувати розмір кола $d_{u\max}$ допустимого переміщення для кожної ТА, як мінімальне значення із всіх $d_{uw\max}$ зі своїми сусідами.

6. Визначити множину можливих місць розміщення ТА в колі переміщення у вигляді решітки точок.

7. Розрахунок пропускної здатності радіоканалів між кожними точками решітки кола можливого переміщення між сусідніми вузлами.

8. Вибір точок решітки з максимальною пропускною здатністю радіоканалів між ТА, як результат рішення – бажане положення ТА.

9. Розрахунок нових пропускних здатностей маршрутів відповідно нових отриманих значень пропускних спроможностей радіоканалів між ТА (вираз 1).

Розрахунок значення пропускної здатності мережі (вираз 1).

10. Перерозподіл вхідного трафіка згідно нових значень пропускних здатностей маршрутів для задоволення його заданого рівня.

11. Перевірка на задоволення вимог вхідного трафіка за радіоканалами та інформаційними напрямами повітряної мережі (нерівності 6 та 4).

ЯКЩО ці нерівності не виконуються, ТО – збільшення зони можливого переміщення ТА за рахунок збільшення до граничних значень довжини маршрутів між наземними вузлами із збереженням зв'язності, які знаходяться за межами зони обслуговування (режим MANET).

ЯКЩО всі варіанти перебрані, але неможливо забезпечити заданий рівень навантаження, ТО – обмеження вхідного трафіка, ІНАКШЕ – перехід до п. 6 з новими точками розміщення ТА.

Обчислювальна складність такого алгоритму дуже значна і дорівнює $O((k\text{-}1)n_{\text{т}u}n_{\text{т}w})$, де $n_{\text{т}}$ – кількість точок можливого розміщення ТА; *u*,*w* – сусідні ТА.

Для скорочення варіантів перебору пропонується ряд евристик, які враховують: взаємне розташування ТА в повітряній мережі, рівень завантаження їх радіоканалів, напрямок розташування конкретної ТА, крок точок розміщення.

1. Для збільшення пропускної здатності радіоканалів, ТА, які знаходяться на краю мережі, повинні вибирати свої точки потенційного розміщення ближче до сусідніх ТА із значним рівнем інтенсивності трафіка в радіоканалах. Так для мережі на рис. 3.2 ТА № 1, 3, 4 бажано розмістити ближче до 2-ої ТА.

2. При наявності перенавантажених радіоканалів доцільно зменшити рівень їх завантаження за рахунок збільшення пропускної здатності цих радіоканалів. Наприклад, для мережі на рис. 1 ТА № 2 повинна вибирати положення, яке дозволить збільшити пропускну здатність перенавантажених радіоканалів у маршрутах передачі 2-3 та 2-4.

3. Для визначення розміру діаметра кола можливого переміщення ТА використовується мінімальне значення із всіх $d_{uw\max}$ зі своїми сусідами. Це доцільно робити, коли сусідні вузли знаходяться у всіх напрямах. Однак, якщо ТА вирішив зменшити відстань з конкретним сусіднім вузлом (вузлами) в певному напряму, то $d_{uw\max}$ розраховується в напрямі цього вузла (вузлів), значення якого може бути значно більшим. Це значно зменшує кількість точок можливого розміщення ТА і кількість варіантів перебору. На рис. 3 дугами показано вибір можливих точок розміщення для ТА № 1, 3, 4. Для вузла 2 необхідно вибирати пріоритетний напрямок скорочення, виходячи з необхідності усунення перенавантаження радіоканалів.

4. Для скорочення варіантів перебору пропонується вибирати крок сітки, який дозволяє отримати збільшення або зменшення швидкості передачі згідно визначеного протоколу та параметрів радіозасобів.

Для оцінки ефективності запропонованого алгоритму пошуку положення ТА для максимізації пропускної здатності ПМ було проведено моделювання за допомогою систем моделювання ns3 при обмеженні: відсутність джерел перешкод поза мережею та застосування моделі розповсюдження радіохвиль у вільному просторі. На прикладному рівні вхідний трафік представлений у вигляді трафіка постійної інтенсивності. Канальний протокол IEEE 802.11.

Були проведені експерименти та отримані залежності приросту пропускної здатності при різних топологіях мережі, різному діапазоні вхідного навантаження та різних розмірностях мережі. Крім цього, проведено моделювання числа ітерацій, необхідних для отримання кінцевого рішення. При застосуванні запропонованого алгоритму пропускна здатність мережі збільшується до 30 %. Більший виграш пропускної здатності досягається при значних величинах зон можливого переміщення вузлів. І виграш зменшується зі зменшенням величини зон можливого переміщення ТА. Приріст пропускної здатності радіоканалів спостерігається в ТА, які знаходяться на окраїні мережі за умови відсутності цільової функції оптимізації пропускної здатності наземних вузлів у зоні обслуговування.

Зі збільшенням роздільної здатності сітки можливого розташування ТА алгоритм визначає позицію ТА близьку до оптимальної. Однак це значно збільшує кількість обчислень. Час виконання алгоритму для 10 ТА і тисяч точок положення ТА не перевищив секунди. Фактично алгоритм працює в реальному масштабі часу та може бути використаний в спеціальному програмному забезпеченні системи управління ТА.

ЛІТЕРАТУРА

1. Степаненко Є.О., Романюк В.А. Задачі синтезу топологій мереж мобільної компоненти з використанням телекомунікаційних аероплатформ. Збірник наукових праць ВІТІ. 2017. № 3. С. 149 – 157.

2. IEEE Std 802.11. IEEE Standard for Information technology – Telecommunications and information exchange between systems. Local and metropolitan area networks – Specific requirements. Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. 2016.

3. Романюк В.А., Степаненко Є.О. Модель позиціонування телекомунікаційної аероплатформи для оптимізації пропускної здатності повітряної мережі. Збірник наукових праць ВІТІ. № 2, 2019. С. 78 – 85.

4. Степаненко Є.О. Модель позиціонування телекомунікаційної аероплатформи для оптимізації пропускної здатності вузлів зони покриття. Збірник наукових праць ВІТІ. 2019. № 1. С. 97 – 104.

Руденко В.І. (ВІТІ)
Бондаренко Л.О. (ВІТІ)
Бузаєва К.О. (ВІТІ)
Остапук О.І. (ВІТІ)

ПЕРСПЕКТИВИ РОЗВИТКУ ТРОПОСФЕРНОГО ЗВ'ЯЗКУ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Актуальність. Застосування систем ультракороткохвильового УКХ радіозв'язку, які побудовані на принципах тропосферного розсіювання, мають ряд унікальних властивостей в порівнянні з іншими родами зв'язку, а саме:

можливість побудови прямих ліній зв'язку між пунктами управління військових формувань через важкодоступні райони та території зайняті противником, без наявності прямої видимості на відстані до 70 – 180 км.;

можливість забезпечення зв'язку на значні відстані без застосування додаткових ретрансляційних станцій (3 – 5 ретрансляцій на лінії довжиною до 800 км.) у порівнянні з радіорелейними лініями зв'язку (до 20 ретрансляцій);

підвищення розвід захищеності ліній зв'язку завдяки значній просторовій вибірковості та високій направленості випромінювання антенних пристроїв;

незалежність якості передачі інформації від характеру бойових дій, погоди, геомагнітної активності, висотних ядерних вибухів, інших дестабілізуючих чинників, які впливають на інші види зв'язку;

можливість побудови комплексів зв'язку в мобільному варіанті (контейнерному та переносному виконанні) при застосуванні сучасних технологій обробки та передачі сигналів;

збільшення економічної доцільності будівництва ліній тропосферного зв'язку (особливо в важкодоступних районах) по відношенню до інших типів ліній зв'язку (проводових, радіорелейних, супутникових);

більш високу пропускну здатність ліній зв'язку по відношенню до систем короткохвильового (КХ) радіозв'язку.

Мета роботи визначення подальшого розвитку тропосферного зв'язку у Збройних силах України.

Постановка задачі. Досвід ведення бойових дій в Афганістані, Сирії, Іраку, в Операції Об'єднаних Сил на сході України показав ефективність використання тропосферних засобів зв'язку в порівнянні з радіорелейними, проводовими та супутниковими засобами. Аналіз розвитку засобів тропосферного зв'язку найбільш розвинутих країн світу свідчить про те, що вони розробляються як інтегровані комплекси, які поєднують в собі режими робіт тропосферного та супутникового, або тропосферного та радіорелейного зв'язку.

Враховуючи те, що Україна не має власної національної системи супутникового зв'язку доцільно проводити розробку нових комплексів тропосферного зв'язку, які б поєднували радіорелейні комплекси прямої видимості (LOS) та загоризонтного розповсюдження радіохвиль (BLOS).

Основні положення. Концепція розвитку військових цифрових тропосферних систем зв'язку ЗС України повинна складатися з наступних напрямків:

1. Створення мобільних комбінованих цифрових тропосферно-радіорелейних станцій для розміщення в контейнерах з режимами роботи LOS, BLOS або їх комбінацій.

2. Застосування – оперативно-тактична і стратегічна ланки управління Сухопутних військ, оперативно-тактична і тактична ланки управління видів ЗС України.

3. Створення переносних комбінованих цифрових тропосферно-радіорелейних станцій з режимами роботи LOS або BLOS.

Основним напрямком розробки сучасних комплексів тропосферного зв'язку має стати вирішення проблем створення інтерфейсів, які здійснюють функції не тільки фізичного і

канального рівня (прийом-передачу і модуляцію-демодуляцію), але і мережевого і транспортного рівнів, тобто формування пакетної структури, маршрутизацію і обробку мультимедійної інформації (мови, відео, даних).

Об’єктом розробки повинна бути не тільки сама система тропосферного зв’язку, але і вся мережева інфраструктура, яка забезпечує безпосередню інтеграцію в існуючі цифрові телекомунікаційні мережі. Практична реалізація таких комплексів тропосферного зв’язку повинна виконуватися на основі модульного принципу побудови з використанням SDR технології і сучасних безпроводових рішень.

Тропосферні станції нового покоління повинні забезпечувати стійку роботу в цифрових мережах з якістю, що визначена в рекомендаціях МСЕ-Т Y.1540, Y.1541 в режимах LOS і BLOS при побудові одноінтервальних і багатоінтервальних ліній зв’язку.

На трасах з тропосферним розсіюванням необхідно застосовувати методи передачі, які придатні для роботи в багатопроменевому каналі із завмираннями. Найбільш привабливим є метод передачі з адаптацією по частоті, який є вдосконаленим різновидом систем з частотним рознесенням сигналів.

Засобами мінімізації впливу багатопроменевості можуть також стати:

рознесення сигналів в просторі і по поляризації;

прийом з використанням еквалайзера;

використання адаптивних багатопозиційних видів модуляції (OFDM, QPSK m-QAM і ін.).

У радіо інтерфейсах інтегрованих комплексів тропосферного зв’язку доцільно застосовувати метод "часового дуплексу", який забезпечить зменшення вартості та масогабаритних показників обладнання, використання всього діапазону частот.

Застосування SDR технології при адаптації параметрів прийомо-передачі до нестабільності середовища поширення радіосигналів при тропосферному розсіюванні має забезпечувати вирішенню наступних завдань:

вибору робочої частоти і ширини смуги частот каналу в момент передачі пакета інформації;

зміни порогового значення шуму на вході приймального пристрою;

вибору схем модуляції;

вибору інтервалу періодичного калібрування сигналу;

вибору режиму захисту кадрів, типу преамбули і захисного інтервалу.

Управління радіорелейно-тропосферною станцією контейнерного і переносного виконання повинно здійснюватися з єдиного для тропосферного та радіорелейного режимів роботи пульта управління.

Функції моніторингу станцій і ліній зв’язку повинні здійснюватися з автоматизованого робочого місця оператора станції з відповідним програмним забезпеченням.

Конструктивне виконання станцій в контейнерному і переносному виконанні повинно передбачати модульність їх побудови з можливістю створення комбінованої станції тропосферного та радіорелейного зв'язку (на основі двох комутованих трансиверів із загальною антеною).

Висновок. Таким чином, створення та впровадження в ЗС України нових цифрових станцій тропосферного зв’язку із застосуванням новітніх інформаційних і телекомунікаційних технологій в значній мірі змінить структуру і принципи побудови системи зв’язку ЗС України та виведе її на більш якісний рівень розвитку.

Руденко М.М. (ВІТІ)
Симоненко О.А. (ВІТІ)

МОДЕЛЬ ОРГАНІЗАЦІЇ СИСТЕМИ ВІЗУАЛІЗАЦІЇ KIBANA В МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

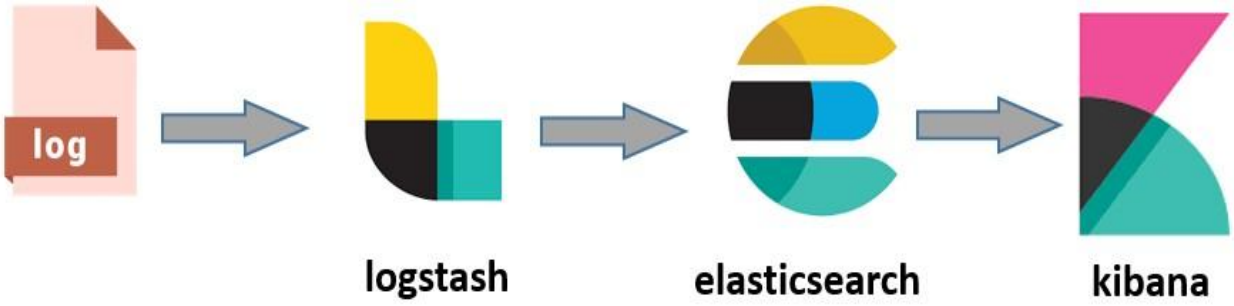
Актуальність дослідження пов'язана з необхідністю забезпечення надійності мереж спеціального призначення, шляхом відслідковування шкідливого трафіку чи несанкціонованого доступу.

Мета. Здійснити аналіз існуючих методів візуалізації та створити модель організації візуалізації *Kibana* на основі кластеру *Elastic*.

Виклад основного матеріалу.

На сучасному етапі розвитку Збройних Сил України, одним з провідних напрямків є впровадження та модернізація новітніх автоматизованих систем управління військами, наприклад „Кропива" та „Дельта". Дані інформаційні системи призначені для полегшення та прискорення процесу прийняття рішень командирами підрозділів на всіх ланках управління. Обов'язковою вимогою коректної роботи такої системи є правильне встановлення та налаштування між елементами системи швидкісних мереж передачі інформації (мереж спеціального призначення). Дуже важливим є те, що такі мережі повинні не лише швидко передавати інформацію, але й відповідати вимогам безпеки. Актуальним рішенням для забезпечення надійності, виявлення неполадок і слабких місць мережі є розгортання серверу, з встановленими програмами *Kibana, Elasticsearch* та *Logstash.*

Даний сервер призначений для збору, аналізу, зберігання та адаптивного представлення інформації, яка міститься в файлах журналювання (*log files*) . Файли журналювання є на всіх мережевих пристроях, в них постійно записується інформація про всі дії, які відбуваються на пристрої. Тобто з'являється можливість відслідковувати надсилання шкідливого трафіку, спроби несанкціонованого доступу, різноманітні атаки на мережу та інше.



Logstash призначений для зчитування інформації одночасно з декількох файлів журналювання. *ElasticSearch* дозволяє шукати потрібні дані по запиту користувача паралельно на безлічі серверів. При цьому дані не обов'язково мають бути структуровані. Також *ElasticSearch* виступає в якості місця зберігання даних. Використовуючи функціонал веб-інтерфейсу *Kibana,* інженер має можливість представити отримані дані з файлів журналювання в різних варіантах оформлення, таких як гістограми, лінійні діаграми, графіки, карти, хмари тегів та інші. Користувач може підібрати необхідні візуалізації для полегшення аналізу даних. Створюючи візуалізації, інженер може побачити дані зі сторони, а також отримати відповіді на питання, які виникають в процесі досліджень.

Висновок: застосування даної моделі з використанням сучасних технологій є актуальним в Збройних Силах України, тому що візуалізація технологічних процесів в мережах спеціального призначення реалізоване не в тому об'ємі, якого вимагає сучасний стан мережі.

Руцький В.О. (ВІТІ)
Троцько О.О. (ВІТІ)

АНАЛІЗ ЗАСОБІВ ВІДДАЛЕНОГО АВТОМАТИЗОВАНОГО УПРАВЛІННЯ МЕРЕЖЕВОЮ ІНФРАСТРУКТУРОЮ

Віддалене управління та обмін інформацією стали основними інструментами роботи системного адміністратора. Програми віддаленого адміністрування – програми або функції операційних систем, що дозволяють отримати віддалений доступ до мережевого обладнання через Інтернет або локальну обчислювальну мережу і здійснювати управління та адміністрування віддаленого мережевого обладнання в реальному часі. Програми віддаленого адміністрування надають майже повний контроль над віддаленим пристроєм.

Існує безліч реалізацій програм віддаленого адміністрування. Всі реалізації відрізняються інтерфейсами і використовуваними протоколами. Програми можуть використовувати графічний інтерфейс користувача (GUI), або інтерфейс командного рядка (CLI). Найбільш популярними і поширеними програмами є компонент Windows Remote Desktop Services з клієнтом Remote Desktop Connection, Radmin, DameWare, PuTTY, VNC, UltraVNC, TightVNC , Apple Remote Desktop, Hamachi, TeamViewer, Remote Office Manager, Ammyy Admin та ін.

Для передачі команд адміністрування та виведення екрана використовуються стандартизовані протоколи віддаленого адміністрування: RDP, VNC, X11, Telnet, Rlogin, RFB, ARD, ICA, ALP, а також пропрієтарні протоколи виробників мережевого обладнання. Для безпечного віддаленого адміністрування використовуються протоколи з шифруванням трафіка SSH, SSL, TLS і ін.

Безпека, надійність і практичність – основні характеристики SSH. Саме це вигідно відрізняє SSH-доступ від інших варіантів управління серверами, інформаційними системами, веб-ресурсами чи обладнанням. Схожий за функціональністю з протоколом Telnet, однак, на відміну від нього, шифрує весь трафік, включаючи і передані паролі. SSH-клієнти і SSH-сервери доступні для більшості мережевих операційних систем. На основі SSH можна не тільки віддалено працювати на комп'ютері через командну оболонку, але і передавати по шифрованому каналу звуковий потік або відео (наприклад, з веб-камери). Також SSH може використовувати стиснення переданих даних для подальшого їх шифрування, що зручно, наприклад, для віддаленого запуску клієнтів X Window System.

Підтримка SSH реалізована у всіх UNIX-подібних системах, і на більшості з них в числі стандартних утиліт присутні клієнт і сервер SSH. Існує багато реалізацій SSH-клієнтів і не для UNIX ОС. Велику популярність протокол отримав після широкого розвитку аналізаторів трафіка як альтернатива незахищеному протоколу Telnet для управління важливими вузлами мережі.

Управління мереж передачі даних, особливо великого розміру, є трудомістким завданням і потребує впровадження засобів автоматизації. Одним з варіантів вирішення цієї задачі є використання програмного забезпечення: Chef, CFEngine, puppet, Ansible.

Ansible – програмне забезпечення, що надає засоби для управління конфігурацією, оркестрування, централізованої установки додатків і паралельного виконання типових завдань на групі систем. З особливостей Ansible можна відзначити просту і легко читану мову управління конфігурацією, підтримку розпаралелювання робіт, відсутність необхідності установки на віддалені системи спеціальних програм-агентів (всі операції ініціюються централізовано по SSH), можливість роботи без прав root. Система Ansible не так ускладнена, як CFEngine, puppet і Chef (програма), але при цьому надає досить широкі можливості і високу гнучкість управління.

Напрямком подальших досліджень є розробка моделі віддаленого автоматизованого управління мережевою інфраструктурою з використанням програмного забезпечення з відкритим кодом Ansible.

к.т.н. Самойлов І.В. (ІСЗЗІ НТУУ „КПІ”)
к.т.н. Застело Г.І. (ІСЗЗІ НТУУ „КПІ”)

ВИКОРИСТАННЯ ЕЛЕМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИДОБУВАННЯ НЕЧІТКИХ ВІДНОШЕНЬ З ЕКСПЕРИМЕНТАЛЬНИХ ДАНИХ

Сучасні технічні системи є складними апаратно-програмними комплексами, що постійно вдосконалюються, розвиваються та модернізуються. Використання таких систем у провідних високотехнологічних сферах (зв’язок, системи управління, телекомунікації тощо) вимагає забезпечення високого рівня надійності їх функціонування. Одним із методів підвищення надійності є розроблення і впровадження ефективних апаратно-програмних засобів діагностування.

На сьогодні актуальною науково-технічною проблемою є створення систем діагностування, які можуть опрацьовувати нечітку діагностичну інформацію. У базах знань таких систем міститься не тільки кількісна інформація, що характеризує стан об’єкта діагностики, а і якісна інформація, яка являє собою експертні оцінки. Однією з задач при проектуванні складних діагностичних систем, є задача створення моделі об’єкта діагностики, яка полягає в побудові оператора зв’язку між причинами та наслідками за експериментальними даними, які є в наявності. В умовах невизначеності для побудови такої моделі зручно використовувати нечіткі відношення і композиційне правило виведення Заде.

При видобуванні нечітких відношень з експериментальних даних нечіткі відношення інтерпретуються як ваги нечітких правил ЯКЩО „причини” ТО „наслідки”. Для отримання цих правил із даних використовуються такі елементи штучного інтелекту, як нейронні мережі або генетичні алгоритми. Недоліком нейро-мережевого підходу є те, що початкова нейро-нечітка мережа містить у собі усі можливі правила. Така мережа містить повнозв’язні шари нейронів, тобто структура моделі не є оптимальною. При цьому конфігурація мережі вимагає, щоб число нечітких термів вхідних і вихідних змінних було строго фіксованим, що обмежує точність нечіткої моделі. Також до недоліків нейро-мережевого підходу слід додати можливість влучення в локальний екстремум. Принциповою перевагою нейронних мереж є здатність адаптивно навчатись по мірі появи нових даних. Перевагою генетичних алгоритмів є те, що вони дозволяють видобувати модель заданої структури. Недоліком генетичного алгоритму є те, що він погано пристосований для врахування нових даних, що надходять у навчальну вибірку.

Комбінація цих елементів штучного інтелекту обумовила появу генетико-нейронних методів видобування знань, суть яких полягає в тому, що генетичний алгоритм використовується для пошуку розв’язку в режимі off-line, а нейронна мережа використовується для уточнення розв’язку в режимі on-line. Пропонується удосконалити генетико-нейронний метод видобування нечітких відношень з експериментальних даних шляхом зміни вектору керувальних змінних на етапах генетичного алгоритму та нейронної настройки.

Таким чином для видобування нечітких відношень з експериментальних даних пропонується використовувати генетико-нейронний метод в якому на відміну від відомих, вектор керувальних змінних на етапі генетичного алгоритму відрізняється від вектора розв’язку на етапі нейронної настройки. Це дозволить на етапі генетичної оптимізації грубо, але швидко визначати розв’язок та оцінювати параметри функцій належності і ваг нечітких правил. Етап застосування нейронної мережі дозволить уточнювати розв’язок і здійснювати його адаптивну корекцію по мірі надходження нових експериментальних даних. Крім того нейро-мережевий підхід забезпечить адаптацію параметрів моделі до варіації вхідних даних, що зумовлені неточністю результатів вимірювань. Подальше підвищення точності моделювання причинно-наслідкових зв’язків, можливо, шляхом параметричної ідентифікації нечітких відношень.

Семенов А.О. (ВІТІ)
Троцько О.О. (ВІТІ)

АНАЛІЗ ДЕСТАБІЛІЗУЮЧИХ ФАКТОРІВ ЩО ВПЛИВАЮТЬ НА ФУНКЦІОНУВАННЯ МЕРЕЖ ПЕРЕДАЧІ ДАНИХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Сучасний стан інформаційних технологій вимагає від мереж передачі даних забезпечення доступності ресурсів у будь-який час, з будь-якого місця та пристрою. Мережі передачі даних спеціального призначення (МПД СП) не є виключенням і повинні забезпечувати доступ до основного об'єму робочих даних і надавати змогу використовувати надійний голосовий та відеозв'язок. Для забезпечення працездатності необхідно створити методику побудови МПД СП з врахуванням чинників які впливають на безперебійну роботу мережі. Для створення моделі необхідно провести аналіз факторів які впливають на мережі передачі даних.

Дестабілізуючі фактори, що впливають на мережі передачі даних спеціального призначення можна класифікувати за наступними категоріями:

За місцем виникнення: зовнішні і внутрішні.

За фізичною природою виділяють такі впливи: звичайна зброя, зброя масового ураження, радіоелектронні засоби боротьби противника, технічні та експлуатаційні відмови, переміщення об'єктів управління, фізично-географічні умови та ін.

За ступенем визначеності: детерміновані (наприклад, планова перебудова телекомунікаційної складової системи зв'язку), імовірнісні з відомими законами розподілу (технічні відмови), імовірнісні з невідомими законами розподілу, невизначені (час нанесення масового удару).

За тривалістю впливу: постійно діючі (ненадійність апаратури), періодичність (вогневе ураження), разові.

За інтенсивністю впливу: слабої, середньої та сильної інтенсивності.

Такий розподіл звичайно умовний і не має чітких меж. Як правило інтенсивність впливу знаходиться у зворотному співвідношенні з його тривалістю.

За проявом: навмисні і випадкові.

Вплив дестабілізуючих факторів на МПД СП поділяється на вплив внутрішніх і зовнішніх дестабілізуючих факторів.

Під внутрішніми дестабілізуючими факторами по відношенню до МПД СП розуміються дестабілізуючі фактори, джерела впливу яких перебувають всередині мережі та є достатня інформація про характеристики їх впливів, що дозволяє приймати ефективні рішення по їх локалізації та проведенню відповідних профілактичних і ремонтно-відновлювальних заходів на всіх етапах, від розробки і виробництва телекомунікаційних засобів до планування та експлуатації МПД СП.

Під зовнішніми дестабілізуючими факторами по відношенню до телекомунікаційної мережі розуміються такі дестабілізуючі фактори, джерела яких розташовані поза даною мережею. Стійкість функціонування МПД СП порушується в результаті впливу перерахованих вище чинників, які через своє різноманіття призводять до того, що забезпечення стійкого функціонування мереж передбачає проведення цілого комплексу організаційних і технічних заходів. Відмова елементів мережі або мережі в цілому є складна випадкова подія, що представляє собою деяку композицію випадкових подій. Різноманітний характер, інтенсивність і закони прояви факторів, які впливають на мережі передачі даних ускладнюють завдання щодо їх урахування, що застерігає від спростованого підходу до дослідження ефективності функціонування МПД СП.

Проведений аналіз дозволить, у ході подальших досліджень, створити методику забезпечення відмовостійкості мережі передачі даних спеціального призначення з урахуванням вище зазначених факторів.

Сердюк П.Є. (ВІТІ)
д.т.н. Слюсар В.І. (ЦНДІ ОВТ ЗСУ)

ТЕХНОЛОГІЇ ДОПОВНЕНОЇ РЕАЛЬНОСТІ – СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ

Технології доповненної реальності для UGV. Перспектива розповсюдження у збройних силах розвинених країн світу різноманітних тактичних засобів доповненої реальності (Augmented Reality, AR) робить актуальною задачею стандартизації відповідної технології візуалізації та протоколів передачі даних.

Слід зазначити, що в залежності від ступеня автономності роботизованої системи можливо кілька варіантів інтеграції AR в відповідний контур управління. Найбільш простий варіант полягає в застосуванні AR в засобах візуалізації інформації оператора UGV, наприклад, шляхом накладення даних AR на відеопотік з бортових камер UGV в обладнанні оператора. Основними напрямками стандартизації AR при цьому є типовою інтерфейс оператора UGV, топологія фреймів візуалізації AR-даних на дисплеях або окулярах AR (фрейм вибору режимів роботи і індикації поточного з них (настройка, бойовий, тренувальний і т.п.); фрейм відображення основної візуальної інформації, фрейм візуалізації даних GPS і параметрів руху безекіпажних платформи, зокрема, за допомогою одного або декількох навігаційних кілець по аналогії з системою ARC4 (США)); типові AR-символи для різних функцій і категорій вирішуваних тактичних завдань; основні технічні специфікації (наприклад, максимальна кількість анотацій, які одночасно виводяться на дисплей і їх щільність на одиницю відстані, принципи фільтрації і агрегації груп символів); протокол передачі AR даних (структура і розміри типового блоку даних). Типовими категоріями анотатівніх тактичних символів для оператора UGV є: положення дружніх підрозділів, передній край і позиції противника, місця знаходження саморобних вибухових пристроїв, дороги, мости, підземна інфраструктура і т.п. Крім того, візуалізації повинні підлягати параметри грунту по трасі руху UGV, віртуальний коридор, розподіл зон ризику вибухобезпеки сусідніх складів боєприпасів відповідно до вимог ESMRM (Explosives Safety Munitions Risk Management) і ін. В перспективі вже в цьому простому варіанті може застосовуватися симбіоз AR с алгоритмами штучного інтелекту (наприклад, Common Objects in Context (COCO)) для формування контурних AR-символів за реальними об'єктами, в тому числі що рухаються, в інтересах розподілу цілевказівки. При підвищенні автономності UGV частина даних AR з мережі управління поля бою (BMS) повинна передаватися на його борт і використовуватися бортовим автопілотом. При цьому можлива попередня завантаження необхідних обсягів AR-даних перед початком виконання місії, а також оперативне їх оновлення на борту UGV в ході виконання поставленого завдання. В цьому випадку потрібно вирішити проблему інтеграції бортових засобів генерації даних AR з архітектурою UGV, а також знайти компроміс в рівні централізації їх підключення до BMS.

Для забезпечення в системі UGV зв'язку великої дальності досить перспективно використання стандартів сімейства IEEE 802.16 WiMax, а також технології LTE. Більш ефективним засобом вважається перехід до використання неортогональної частотного мультиплексування сигналів (N-OFDM). Це дозволить враховувати значення амплітудно-частотних характеристик фільтрів, синтезованих за допомогою операції швидкого перетворення Фур'є на частотах, що піднесуть, зміщених через ефект Доплера.

З урахуванням зазначених обставин практичний інтерес може представляти застосування бесквадратурной аналогової обробки сигналів з подальшим формуванням квадратурних складових напруг в цифровому вигляді на основі використання цифрових I/Q-демодуляторів.

ВИСНОВОК. Зазначена спільність підходів до забезпечення каналів зв'язку з БПЛА та UGV є ключовим фактором, що сприяє зниженню вартості відповідного обладнання і розширення функціональних можливостей безекіпажних платформ різного призначення.

к.т.н. Сидорчук О. Л. (ЖВІ)
Кліменко Д.О. (ЖВІ)
Дворський В. О. (ЖВІ)

МАЛОГАБАРИТНИЙ РУПОРНИЙ ОПРОМІНЮВАЧ ДЗЕРКАЛЬНИХ АНТЕННИХ СИСТЕМ СТАНЦІЙ РАДІОТЕХНІЧНОЇ РОЗВІДКИ

В умовах сучасних інформаційних, телекомунікаційних і радіо-технологій у системах військового і державного керування актуальними є задачі забезпечення стійкого функціонування антенних систем засобів зв'язку з позиції їх електромагнітної сумісності та захисту від технічних засобів розвідки противника.

У доповіді пропонуються спроби впровадження нових, захищених патентами на винахід конструктивних рішень, які дозволять забезпнечити таке функцонування, зменшити радіолокаційну помітність антенних систем радіоелектронних засобів та покращити їх електромагнітну сумісність. Для вирішення поставленого завдання пропонується два варіанти нових конструкцій антен.

Перший варіант це малогабаритна рупорна антена з конусоподібним поглиначем вищих гармонік (патент на винахід № 96661 від 13.07.2011). В основу винаходу поставлено задачу вдосконалення рупорної антени колової поляризації. На відміну від прототипів запропонована конструкція має діелектричний конус з поглинаючими канавками, прикріплений до поглинаючої пластини. Для створення колової поляризації встановлено фазуючу секцію, яку виконано у вигляді трапецієподібної діелектричної пластини та розміщено по діагоналі квадратного відрізка хвилеводу. Поглинаючі канавки можуть бути заповнені будь яким градієнтним матеріалом, проте для проведення експерименту використано хром та звичайну сажу.

Експеримент показав, що завдяки введенню додаткового хвилеводного навантаження у вигляді діелектричного конуса з поглинаючими канавками зменшується рівень відбитої хвилі, що призводить до зменшення ефективної поверхні розсіювання (ЕПР) антени. Фазуюча трапецієподібна діелектрична пластина, окрім утворення колової поляризації, поліпшує узгодження хвилеводу з довгими неоднорідними гантелеподібними щілинами. Таким чином запропонована антена працює в широкій смузі частот (більше 35%), має добре узгодження двох довгих неоднорідних гантелеподібних щілин з відрізком квадратного хвилеводу і малу ЕПР. Експериментальні дослідження запропонованої антени у діапазоні 8-12 ГГц довели, що ЕПР було зменшено на 12 дБ. Діаграма спрямованості становила 55°–65° на рівні 0,5 за потужністю, коефіцієнт еліптичності складав 0,82–0,85 дБ. Коефіцієнт стоячої хвилі за навантаженням коливався 1,25–1,3, а втрати становили 0,5–0,7 дБ.

Другий варіант це рупорна антена зі зменшеною ЕПР від кромок (патент № 97037 від 26.12.2011). Проведено експериментальні дослідження запропонованої конструкції антени у діапазоні 8–12,5 ГГц. Для виділення відбитого сигналу на фоні завад (відбиттів від предметів, що знаходяться поруч) використано ефект зміни частоти через рух джерела електромагнітного випромінювача, що дозволило значно зменшити вплив відбиття від нерухомих об'єктів і виключити вплив випадкових варіацій. За проведеними вимірюваннями з'ясовано, що, у порівнянні з прототипом, ЕПР нової конструкції в області головної пелюстки діаграми розсіювання було знижено з 20 дБ до 12 дБ.

В результаті експериментальних досліджень доведено, що найбільш ефективними щодо зниження радіолокаційної помітності антен, є способи, що пов'язані зі зменшенням коефіцієнта стоячої хвилі у колі навантаження та зниженням рівня бічних пелюсток діаграми спрямованості антен на частотах основного і небажаного випромінювань. Вноситься пропозиція щодо заміни штатних опромінювачів антенних систем на розглянуті конструкції, що дозволять покращити якість функціонування самих станцій та їх електромагнітну сумісність з іншими радіоелектронними засобами за рахунок зниження енергетичних втрат.

к.т.н. Сидорчук О. Л. (ЖВІ)
Левунець Р. О. (ЖВІ)

ДОСЛІДЖЕННЯ ЕЛЕКТРОМАГНІТНОГО ПОЛЯ ДЛЯ ПРОЕКТУВАННЯ ДЗЕРКАЛЬНИХ АНТЕННИХ СИСТЕМ СТАНЦІЙ РАДІОТЕХНІЧНОЇ РОЗВІДКИ

Задача підвищення ефективності роботи радіотехнічних станцій (РТС) особливо при виявленні та ідентифікації складних видів сигналів може бути вирішена за умови отримання додаткових ознак. У системі розпізнавання сигналів можуть бути використані портрети сигналів, що ґрунтуються на різноманітних ознаках: флуктуаційних, частотно-кореляційних, частотно-резонансних, поляризаційних, тощо.

Оскільки інформація про ознаки утримується у приймальних сигналах, що є результатом взаємодії зондуючих сигналів з об'єктом, то одним із шляхів отримання додаткових ознак може бути використання зондуючих сигналів на ортогональних, або коловій поляризаціях.

Варіантом побудови антенної системи, що забезпечує випромінювання сигналів на двох ортогональних поляризаціях, може бути дзеркальна параболічна антена. Її перевагою є можливість формування високого енергетичного потенціалу радіолінії при відносній невисокій, по відношенню до інших антенних систем, вартості антени.

Для проектування та побудови таких антен необхідно визначитись із методом знаходження дифракційного поля дзеркальної антени колової поляризації.

У доповіді пропонується розв'язання задачі розрахунку електромагнітного поля в області параболоїда обертання і визначення дифракційного поля дзеркальної антени з рупорним опромінювачем колової поляризації.

Подібна задача вже вирішувалась для однополяризаційної дзеркальної антени. Дифракційне поле знаходилось у такій послідовності: після визначення поля в області фокуса, знаходилось поле, перевідбите від рупорного опромінювача, яке, падаючи знову на дзеркало, створювало перевідбите поле вже від усієї антени в дальній зоні. В інших роботах розглядалось поле в області фокуса параболоїда обертання при пряму падінні на нього плоскої електромагнітної хвилі. Довільне падіння електромагнітної хвилі не розглядалось.

У доповіді пропонується метод визначення електромагнітного поля, розсіяного від рупорної антени колової поляризації, розміщеної в площині фокуса параболоїда обертання при падінні на неї довільно падаючої плоскої електромагнітної хвилі.

Новий метод базується на тому, що загальний випадок довільного падіння плоскої електромагнітної хвилі розглянуто як суперпозицію двох окремих випадків: хвиля поляризована нормально до площини падіння та хвиля поляризована в площині падіння. Поставлена задача включає в себе дві складові:

а) визначення поля в площині фокуса параболоїда обертання при падінні на нього довільно падаючої плоскої електромагнітної хвилі;

б) визначення розсіяного поля від рупорного опромінювача колової поляризації, розміщеного в площині фокуса параболоїда обертання при падінні на нього довільно падаючої плоскої електромагнітної хвилі.

Розрахунки за новим методом дозволять судити про вплив різноманітних елементів, розміщених в площині фокуса на розсіяння дзеркальної антени з рупорним опромінювачем РТС в цілому при будь якому випадку падінні хвилі на дзеркало.

Побудова РТС на основі такої антени, при використанні сучасних апаратно-програмних засобів цифрової обробки прийнятих сигналів, дозволить отримати значні переваги над традиційними однополяризаційними антенними системами при виявленні сигналів і виділенні їх інформативних ознак.

Симоненко О.А. (ВІТІ)
Білан А.М. (ВІТІ)
к.т.н Жук О.В. (ВІТІ)

КІБЕРТЕРОРИЗМ У КОНТЕКСТІ ПОБУДОВИ СИСТЕМИ КІБЕРНЕТИЧНОГО ЗАХИСТУ ДЕРЖАВИ

Збройні конфлікти сучасності охоплюють не тільки традиційні сфери збройної боротьби, зокрема землю, повітря, море, а й поступово просуваються у такі сфери, як інформаційний та і кібернетичний простори. Зокрема „кібернетичний простір" розуміється як складова національної інформаційної структури, яка становить сукупність інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем (мереж) загального користування та Національної критичної інформаційної інфраструктури у т.ч. спеціальних телекомунікаційних систем (мереж). Похідним цього визначення є „кібернетична безпека", яка тлумачиться як стан захищеності кібернетичного простору в цілому або окремих його складових, при цьому забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація кібернетичних загроз, зокрема кібертероризму.

Особливі ознаки кібертероризму:

– анонімність джерела кібератаки;

– глобальний характер та висока ефективність;

– тимчасова невизначеність у часі як самої кібератаки, так і процесу її Підготовки;

– можливість організації складних кібератак одночасно на різні об'єкти з різних напрямів;

– анонімність злочинця;

– зниження морально-психологічного тиску на суб'єкта кібератаки, пов'язане з просторово-часовою віддаленістю від об'єкта кібератаки.

Розв'язання проблеми протидії кібертероризму грунтується на комплексному підході та має такі складові, як:

– *правова* – пов'язана з розробленням нормативно-правових актів, які регламентують відносини в інформаційній сфері, і нормативно-методичних документів із питань забезпечення інформаційної безпеки;

– *організаційна* – полягає в удосконаленні організаційної структури державних і комерційних підприємств, сертифікації і стандартизації засобів захисту інформації та ліцензуванні діяльності із захисту інформації;

– *психологічна* – передбачає формування високих морально-етичних норм у співробітників, які працюють з інформаційними системами, що забезпечують критичну інфраструктуру держави;

– *технічна* – ґрунтується на створенні й постійному вдосконаленні системи забезпечення інформаційної безпеки на об'єктах інформатизації та попередження нападу.

Підсумовуючи викладене, слід зазначити, що кібертероризм – нова загроза інформаційному суверенітету держави. Це питання є недостатньо дослідженим, що перешкоджає оперативному реагуванню на скоєння комп'ютерних злочинів. Проблему також загострює нагальна потреба у досвідчених фахівцях із питань захисту інформації та протидії кіберзлочинності. Тому сьогодні одним із першочергових завдань виступає належна організація процесу забезпечення національної системи інформаційної безпеки висококваліфікованими фахівцями з урахуванням певних особливостей цієї сфери, а саме:

– система освіти в галузі інформаційної безпеки має забезпечувати відповідність рівня підготовки фахівців темпам розвитку науково-технічного прогресу та відповідного національного законодавства;

– система підготовки ІТ-фахівців потребує проведення обов'язкового контролю та моніторингу;

– стан інформаційної безпеки визначається не тільки рівнем підготовки, а й перепідготовки (підвищення кваліфікації) фахівців у цій сфері.

д.т.н. Слюсар В.І. (ЦНДІ ОВТ ЗСУ)

КОНЦЕПЦІЯ АРХІТЕКТУРИ ТРАНСПОРТНИХ ЗАСОБІВ ЯК МЕРЕЖІ МЕРЕЖ

Важливою умовою ефективного ведення бойових дій є скорочення часу реакції систем озброєння і підвищення швидкодії усіх підсистем бойових транспортних платформ (пілотованих та безекіпажних). В критично важливих випадках мова йде про час реакції у наносекунди, особливо це стосується бортових систем пожежогасіння, активного броне- та протимінного захисту. В умовах мережної побудови транспортних засобів на основі стандартизованої архітектури, наприклад, NGVA (NATO Generic Vehicle Architecture), можливим рішенням було б застосувати на борту транспортної платформи високошвидкісну мережу, наприклад, зі швидкістю трафіку 100 Гбіт/с. Однак порівняно великі відстані для передачі сигналів (в межах бойової машини це кілька метрів) робить реалізацію такої мережі технічно складною проблемою, й до того ж досить дорогим рішенням. Тому в якості компромісу слід розглянути створення багатомережного конгломерату, що являє собою сукупність кількох функціонально відмінних мереж з різною швидкодією [1].

Метою доповіді є обґрунтування мультимережної концепції NGVA як альтернативи стандартизованій в НАТО одномережній архітектурі транспортних засобів (STANAG 4754).

Відомо, що консорціум компаній на чолі з Leonardo (Велика Британія) має наміри реалізувати до 2020 року технічну демонстраційну програму (TDP) Icarus стосовно створення модульної інтегрованої системи активного захисту (Modular Integrated Protection System, MIPS) з відкритою модульною архітектурою (Modular Open System Architecture, MOSA). Програма передбачає адаптацію системи активного бронезахисту (DAS) для цілої низки різних платформ з інтеграцією до загальної архітектури транспортних засобів (GVA). Суттєво, що ця робота пов’язана, але не перекривається з STANAG 4686 щодо випробувань та визначення рівнів продуктивності DAS, а також з NGVA.

При традиційному підході система DAS використовує інформацію від систем транспортної платформи, а це не дозволяє оптимізувати спроможності системи активного бронезахисту, яка має працювати у реальному масштабі часу (інтервал від виявлення до ураження загрози має не перевищувати 100 мс). Крім того, інформація від сенсорів DAS повинна поступати в інформаційну систему транспортної платформи, наприклад, для відображення за допомогою технології доповненої реальності на моніторі командира тих блоків DAS, що вже спрацювали. В рамках проекту Icarus вивчаються різні конфігурації, коли сенсори і засоби ураження DAS підключають до NGVA або в окрему більш швидкісну мережу, що поєднана з NGVA через окремий шлюз (запропоновано автором на засіданні групи НАТО з розвитку спроможностей ведення наземного бою (LCG LE) у квітні 2018 р.).

Випробування технічного демонстратора Icarus плануються на 2020 рік. Зараз на основі методології системного інженерінгу відпрацьовуються перелік випадків використання (use cases), модель даних, спроможності автоматичного кодування, відповідні вимоги з потребою захисту від атак БПЛА та реалізації комплексних сценаріїв захисту з одночасним відбиттям атаки ПТРК (ATGM) і, наприклад, підкаліберних снарядів.

Слід звернути увагу на схожість завдань активного бронезахисту з пожежогасінням. Отже, у складі NGVA можливо функціонування як мінімум двох мереж реального часу. Тому для наступної редакції стандарту на архітектуру транспортних засобів NGVA доцільно розглянути мультимережну концепцію NGVA як мережу мереж з різними швидкостями обміну даними, в якій мережі реального часу зі швидкістю трафіку, наприклад, 10-40 Гбіт/с (активний бронезахист, пожежогасіння, активний захист від підриву мін тощо), а також більш повільні мережі підключені через шлюзи до основної мережі, що функціонує на швидкості до 1 Гбіт/с (стандартизована в НАТО швидкість передачі відеоданих в машині) й здійснює управління рештою мереж.

З огляду на це, розробку стандарту на відкриту архітектуру активних систем бронезахисту доцільно розглядати як проміжний етап на шляху до зазначеного поновлення

концепції NGVA. В подальшому необхідно буде включити до Land Data Model NGVA як складову частину MIPS Sytem Model та її компоненти: MIPS Data Model (розробляється аналогічно NGVA Data Model), MIPS Time Sensitive Data Model та ін.

В якості механізму поширення інформації в мультимережній системі транспортного засобу доцільно обрати комбінацію DDS (Data Distribution Service) та MQTT (Message Queuing Telemetry Transport), яка запропонована в [2] для Інтернету речей (IoT). Основну бортову мережу транспортної платформи, що має виконувати функції централізованого мультимережного менеджменту, пропонується реалізувати на основі MQTT та передбаченого цим протоколом брокерського механізму. Більш швидкісні мережі транспортного засобу повинні спиратися на технологію DDS, яка завдяки децентралізації дозволяє максимально мінімізувати час затримки на проходження повідомлень й тому отримала поширене застосування при вирішенні завдань у масштабі реального часу. Мережі з відносно повільною передачею даних, наприклад, бортова мережа солдат (Soldier System Network), що транспортуються закріпленою за ними бойовою машиною [3], можуть сполучатися також на основі транспорту даних MQTT. Це дозволить автоматично вирішити й проблему несанкціонованого доступу до відповідної мережі передачі даних, голосової комунікації та електроживлення.

Разом з тим, від традиційних для DDS затримок на проходження даних (кілька сотен мкс на 1 мс) у бортових мережах реального часу необхідно перейти до затримки у наносекунди. Це досягається підвищенням частоти синхросигналів мереж і важливо, наприклад, для реалізації бортової системи пожежогасіння, а також інтегрованої до модульної архітектури системи активного захисту від підриву мін, на зразок тієї, що пропонується компанією Tencate. При цьому необхідно здійснити пошук компромісу між кількістю адресатів в окремій мережі (сенсори, виконавчі модулі, блоки управління) та її швидкодією з одної сторони, а також кількістю бортових мереж – з іншої.

Запропонована багатомережна концепція на даному етапі є менш дорогим технічним рішенням і дозволяє підвищити стійкість мережної архітектури до впливу відмов внаслідок вогневого ураження противником.

Спираючись на такий підхід, слід розширити асортимент підключених до базової мережі NGVA мереж реального часу, при цьому доцільно використовувати для кожної підмережі один або кілька шлюзів, з розрахунку один шлюз на мережевий сегмент. Ідея смарт-шлюзів має сенс тільки в рамках сполучення мереж порівнянної продуктивності. Очевидно, якщо не брати до уваги багатосерійний випуск, немає сенсу застосовувати високошвидкісний шлюз на 100 Гбіт/с для сполучення між собою мереж з трафіком 1 Гбіт/с. Поняття „смарт” у відношенні шлюзів в цьому випадку буде мати на увазі їх автоматичну функціонально-сигнальну адаптацію.

ЛІТЕРАТУРА

1. Слюсар В.И. Концепция мультисетевой архитектуры транспортных платформ.// 15-а наукова конференція Харківського національного університету Повітряних Сил імені Івана Кожедуба. – Харків: ХНУПС. – 10 – 11 квітня 2019 р. – С. 355. – http://slyusar.kiev.ua/HNUPS_2019.pdf.

2. David Barnett. Comparison of MQTT and DDS as M2M Protocols for the Internet of Things. Published on May 29, 2013. – https://www.slideshare.net/RealTimeInnovations/comparison-of-mqtt-and-dds-as-m2m-protocols-for-the-internet-of-things.

3. Слюсар В.І. Інтеграція архітектур транспортних засобів (NGVA) та систем військовослужбовця (DSRA). //17-а науково-технічна конференція “Створення та модернізація озброєння і військової техніки в сучасних умовах”.– Чернігів: Державний науково-випробувальний центр Збройних Сил України. – 07 – 08 вересня 2017 р. – С. 332 – 333. – http://slyusar.kiev.ua/Slyusar_DNVC1.pdf.

Слюсар Є.А. (ВІТІ)
Редзюк Є.В. (ВІТІ)

ПРОГРАМНИЙ МОДУЛЬ АНАЛІТИЧНОЇ ОБРОБКИ ДАНИХ УСПІШНОСТІ НАВЧАЛЬНИХ ГРУП

Актуальність дослідження пов'язана з необхідністю у вдосконаленні системи підготовки якісних офіцерських кадрів та оцінювання успішності. Необхідна для цього система з можливістю перегляду повної статистики по успішності навчання як групи в цілому, так і окремих курсантів, можливість порівняти якості навчання декількох груп (окремих курсантів), визначення більш складних занять та занять, вивчення матеріалів яких не викликала труднощів, не була розроблена, а виконувалася за допомогою ручних обрахунків. Для вирішення цього завдання розроблено програмний модуль аналітичної обробки даних успішності з навчальних дисциплін ВВНЗ, що надасть допомогу як викладачу у відсутності „паперової" роботи, так і курсанту для відстеження статистики свого навчання.

Для досягнення поставленої цілі було сформовано низку задач:

−генерування основних вимог до програмного модулю та підготовка до роботи;

−розробка програмного модулю та оцінка його ефективності.

Мета роботи полягає в розробці програмного модулю аналітичної обробки даних успішності навчальних груп.

Основні положення. Дані – це формалізоване подання інформації, придатне для інтерпретування, пересилання чи оброблення за участю людини або автоматичними засобами. Дані самі по собі не є інформацією. Інформацією стають оброблені та інтерпретовані за заздалегідь узгодженою схемою дані. Інколи дані описують іншими даними. Знання головних питань описової статистики є головними для аналітичної обробки даних. Аналіз даних вміє давати загальні характеристики для великих вибірок, може проводити порівняння між різними вибірками, а також аналіз даних можна використовувати для встановлення структури. Для розробки програмного модуля та виконання поставленого завдання використаємо мову програмування для статистичних обчислень *R* та мову програмування третього покоління *C#*.

Програмний модуль вміщує в собі:

−розроблений за допомогою мови статистичного аналізу, блок аналітичної обробки, в якому описані всі методи статистичного аналізу, необхідні для виводу повної інформації про успішність навчальних груп та курсантів в цілому;

−блок завантаження даних, який містить в собі функціонал для завантаження дата фреймів з отриманими оцінками;

−блок візуалізації для відображення графічної обробки даних;

−для комфортного користування програмного модулю було створено блок роботи з користувачем для внесення необхідних для нього даних;

−блок керування для взаємодії між іншими блоками програмного модулю;

−блок збереження завантажених даних.

Розроблений програмний модуль виводить детальну статистику про успішність курсантів навчальних груп з різних дисциплін на основі набраних балів на протязі навчального семестру. Також містить можливість порівнювати статистику успішності навчальної групи за кожен навчальний рік, виводить процес успішності кожного курсанта, як за допомогою цифр так і за допомогою графікі та порівнювати успішність групи з різних дисциплін. Програмний модуль має зручний та зрозумілий інтерфейс для роботи з користувачем. **Висновки.** Отже, даний програмний модуль значним чином полегшує аналітичну обробку успішності навчальних груп з різних дисциплін, а також окремих курсантів та є більш ефективним та значно заощаджує час порівняно з ручними обрахунками. Даний програмний модуль був розроблений з метою полегшення роботи при аналізі успішності навчальних груп ВВНЗ.

к.-ф.-м.н. Сокульська Н.Б. (НАСВ)
д.т.н. Сокіл Б.І. (НАСВ)
к.т.н. Ковальчук Р.А. (НАСВ)
Кмін В.Ф. (НАСВ)

ДИСТАНЦІЙНЕ НАВЧАННЯ ЯК ОДИН ІЗ НАПРЯМІВ ВДОСКОНАЛЕННЯ ПІДГОТОВКИ ВІЙСЬКОВИХ ФАХІВЦІВ

Актуальність. Питання упровадження в навчальний процес ВНЗ інноваційних педагогічних технік і методів шляхом залучення новітніх інформаційних технологій є одним із пріоритетних шляхів модернізації освітньої системи. У зв'язку з масовим застосуванням у навчальному процесі персональних комп'ютерів та комп'ютерних систем останні набули нового розвитку. Інформатизація освіти є комплексом заходів, пов'язаних із використанням інформаційних засобів та інформаційної продукції. Про необхідність введення в освітнє середовище інноваційних методик на базі нових технологій, в основу яких покладені цілісні моделі навчально-виховного процесу, засновані на діалектичній єдності методології та засобів їх здійснення в цілому, йдеться, зокрема, в роботах О. Торубари, Н. Дудник, О. Брусєнцевої, Р. Гуревича, Н. Буги, І. Дичківської. Проте, досі маловивченими залишаються питання застосування інноваційних методів навчання, базованих на новітніх технологіях, у вищих військових закладах, зокрема через специфіку викладання та навчання в ВУЗах даного типу. Авторами розглядаються особливості впровадження дистанційного навчання в сучасну систему військової освіти на прикладі викладання вищої математики та інженерних дисциплін, пов'язаних з нею, їх правове підґрунтя, та суспільні виклики, що диктують необхідність такого впровадження. розглянуті вибрані моделі і технології дистанційного навчання, що вводяться у військових вузах. Вказано на ряд їх переваг. Наголошено на проблемах їх впровадження в освітній процес.

Метою роботи є аналіз впровадження у підготовку військових фахівців Національної академії сухопутних військ ім. гетьмана Петра Сагайдачного дистанційного навчання на базі платформи „MOODLE", його переваги та недоліки.

Основні положення. Відповідно до вимог сьогодення Міністерством освіти було прийнято Положення про дистанційне навчання, яким визначаються основні засади організації та запровадження такого навчання. Керуючись ним, Міністерство Оборони своїм наказом затвердило Концепцію (далі – Концепція) Дистанційного навчання (ДН) у Збройних силах, метою якої є „наближення військової освіти до сучасних вимог та перспектив розвитку теорії і практики збройної боротьби". Дана модель покликана забезпечити:

– виникнення нових можливостей для оновлення змісту навчання та методів викладання дисциплін і поширення знань;

– розширення доступу до навчальних ресурсів, реалізацію можливості навчання без обмежень за просторовою та часовою ознаками, з мінімальним відривом від виконання професійних обов'язків;

– індивідуалізацію навчання»

Відповідно до положень Концепції. Дистанційна форма навчання „… може бути застосованою у поєднанні з очною, заочною формами навчання… ", що здійснюється з використанням програмного забезпечення „…для створення, збереження, накопичення та передачі веб-ресурсів, забезпечення авторизованого доступу суб'єктів ДН до цих веб-ресурсів, а також організації навчального процесу і контролю за навчанням через Інтернет та/або локальну мережу."

Міністерством Оборони для втілення цієї концепції було прийнято рішення впроваджувати ДН на основі платформи „MOODLE". Навчання на базі платформи має ряд переваг.

По-перше, його можна здійснювати віддалено і в зручний для слухача час.

По-друге, тут існує можливість встановлювати чіткі часові рамки для здійснення певних видів діяльностей, відслідковувати їх виконання, спонукати до послідовного ознайомлення з матеріалом дисципліни.

По-третє, здійснювати перевірку набутих знань можна як і через написання рефератів, есе, так і за допомогою різноманітних тестів, що сприяє об'єктивності оцінювання.

По-четверте, в нових версіях даної платформи існує можливість встановлення відеоконференції між викладачем та слухачами як для проведення навчання так і для зворотного зв'язку від слухача до викладача.

На даному етапі в НАСВ лише впроваджується та тестується навчання на базі платформи «MOODLE» Міністерства Оборони (глобальної), але цілком можливо використовувати наповнення дисциплін «локальної» (мережі дистанційного навчання в межах території навчальних корпусів Академії) платформи «MOODLE», що впроваджена тут кілька років тому. Специфіка навчання курсанта Академії передбачає систему т.з. нарядів, тобто його чергування на певних пропускних та інших пунктах. Тому доволі часто слухачі не мають можливості навчатись разом з групою. Таким чином, курсанти надолужують пропущений матеріал, та використовують ресурси цієї платформи для самопідготовки, опрацювання пропущеного матеріалу.

Крім того, дані платформи зручно використовувати з метою об'єктивності оцінювання, оскільки тут можна проводити різного типу тестування, контрольні заходи, зрізи знань.

При викладанні та вивченні дисциплін математичного циклу таких, як вища математика, теоретична механіка та прикладна механіка, опір матеріалів, тощо, всі вище перераховані переваги знаходять місце.

Але попри те викають і певні суттєві недоліки.

Перш за все, при роботі з аудиторією в класичний спосіб викладач математики може зрозуміти, чи слухачі сприймають новий матеріал, чи їм потрібно навести додаткові відомості з базового курсу для кращого сприйняття цього матеріалу, а вже при роботі, навіть, в режимі реального часу з слухачами дистанційного курсу таке «відчуття аудиторії» втрачається. По-друге, при онлайн-тестуванні, чи інших формах дистанційного опитування існує більше можливостей до певного роду махінацій з боку слухачів. Тому будь-яку дистанційну форму доцільно поєднувати і з очними формами контролю. Третьою проблемою є неадаптованість систем платформи для зручного введення та конвертації формул та математичних співвідношень, що значно ускладнює викладачеві математичних дисциплін процес наповнення дистанційного курсу.

Висновки. Загалом, пілотний проект з навчання військових фахівців з використанням платформи дистанційного навчання ЗСУ MOODLE, що здобувають освіту в Академії заочно, стартував. На даному етапі усі його переваги та недоліки, що виникли під час викладання, вищої математики, вказані вище, а повноцінно про його якість можна буде зробити висновки за результатами сесії.

Використання ж «локальної» мережі MOODLE доволі обмежене рядом технічних особливостей. Зокрема, через певну таємність в Академії користуватись даними ресурсами можна лише з обмеженої захищеної кількості комп'ютерів, доступ до якої, на жаль, мають не усі курсанти. Але вже зараз її використовують для проведення зрізів знань з математики та механіки.

Як показує практика, у групах, де був здійснений контроль таким чином, спостерігається різке пожвавлення серед курсантів, виникає зацікавлення питаннями, зав'язується дискусія.

В результаті слухачі отримали більше інформації, вчилися: аналізувати почутий матеріал, критично мислити, відкидати неважливе; набувати навичок швидко приймати рішення, що є доволі важливою характеристикою військового офіцера.

Солодовник В.І. (ВІТІ)
Висоцька Т.М. (ВІТІ)
Османов Р.Н. (ВІТІ)

ОЦІНКА ЗАВАДОСТІЙКОСТІ МЕТОДІВ ПРОСТОРОВОГО КОДУВАННЯ СИГНАЛІВ З ДВОРЕЖИМНОЮ ІНДЕКСНОЮ МОДУЛЯЦІЄЮ ПІДНЕСУЧИХ

Однією з основних вимог до сучасних систем безпроводового зв'язку спеціального призначення (СБЗСП) є підтримка об'ємних інформаційних мультимедійних додатків із забезпеченням високих показників завадостійкості та швидкості передачі інформації. В умовах складної завадової обстановки, під впливом засобів радіоелектронного подавлення (РЕП) високоефективне використання реальних безпроводових каналів зв'язку суттєво ускладнюється через їх частотну селективність та нестаціонарну поведінку, а також обмеженість частотно-енергетичних та просторових ресурсів.

На теперішній час найбільш продуктивним методом забезпечення високої інформаційної, енергетичної (ЕЕ) та спектральної ефективності (СЕ) сучасних СБЗСП є технологія сумісного застосування багатоантенних систем (Multiple Input-Multiple Output, MIMO) та ортогонального частотного розподілу каналів з мультиплексуванням (Orthogonal Frequency Division Multiplexing, OFDM). Технологія MIMO-OFDM є невід'ємною частиною практично всіх стандартів безпроводового зв'язку: LTE, LTE-A, WiMAX та Wi-Fi. Найбільш широкого застосування знайшли методи ортогонального просторово-часового (Space-Time Block Coding, STBC) та просторово-частотного блочного кодування сигналів (Space-Frequency Block Coding, SFBC) для двох передавальних антен. Обидва варіанти рознесеної передачі сигналів за принципом Аламоуті (часовий (STBC) та частотний (SFBC)) мають мінімальну довжину кодового слова, що позитивно впливає на забезпечення квазістаціонарності каналу в умовах частотно-часової селективності. Однак методи STBC та SFBC потребують удосконалення як в частині підвищення СЕ, так і ЕЕ, насамперед, при низьких співвідношеннях сигнал/шум (Signal-to-Noise Ratio, SNR), що мають місце при інтенсивній роботі засобів постановки навмисних завад.

Традиційні шляхи підвищення СЕ та ЕЕ, пов'язані зі збільшенням швидкості модуляції, об'єму ансамблю сигналів, кількості антен та потужності випромінювання, вичерпали себе через частотно-енергетично-просторову обмеженість безпроводового каналу зв'язку. Збільшити швидкість передачі цифрової інформації можливо завдяки введенню додаткових сигнальних вимірів, що забезпечують формування та передачу певної частини інформаційних біт шляхом реалізації неявного інформаційно-керованого механізму перемикання стану активності допоміжних блоків передачі.

В останнє десятиліття розроблено широкий клас схем з індексною модуляцією (Index Modulation, IM), в яких інформаційні біти можуть приєднуватись до різних фізичних або віртуальних блоків трансляції. Індексна модуляція – це методи передачі інформації, що полягають у поділі інформаційних біт на індексні та біти символів ансамблю сигналів з подальшою активацією елементів блоків, що передають ці символи. Оскільки метод OFDM став практично безальтернативним способом боротьби з міжсимвольною інтерференцією (Inter-Symbol Interference, ISI), тому для класу частотно-селективних каналів найбільш привабливим є метод індексної модуляції піднесучих OFDM (OFDM-IM), що дозволяє одночасно підвищити завадостійкість та швидкість передачі інформації за рахунок введення додаткового частотного виміру сигналів.

Оцінку завадостійкості сигнально-кодових конструкцій (СКК), побудованих шляхом сумісного застосування індексної модуляції піднесучих OFDM та часової (або частотної) версії коду Аламоуті, проведено з використанням комп'ютерної моделі у середовищі MATLAB Simulink. Вхідними даними моделі є: кількість передавальних та приймальних антен (MIMO 2×1 та 2×2); вид модуляції (BPSK, QPSK та 16-QAM); кількість піднесучих OFDM (256); довжина послідовності генератора цифрового потоку ($2\cdot10^6$ біт); максимальне

число помилок на виході декодера (≥ 200). Використана для моделювання схема релеївських завмирань найбільш повно характеризує багатопроменеве розповсюдження сигналів у безпроводовому каналі зв'язку за відсутності прямої видимості між передавачем та приймачем або в умовах щільної міської забудови. Обрано дві моделі каналів у залежності від рівня частотної селективності: величина середньоквадратичного значення затримки τ = 1,43 мкс характеризує канал з помірною (ПС) селективністю, а τ = 9,91 мкс – канал з високим (ВС) рівнем селективності. Підвищення рівня нестаціонарності каналу значно погіршує завадостійкість системи передачі інформації. Обрані для моделювання значення нормованого доплерівського зсуву частот $F_{\text{Д}} = f_{\text{Д}} \cdot T_{symb} = 0{,}01...0{,}05$ ($f_{\text{Д}} = 100...500$ Гц) відповідають швидкості руху мобільної станції 45 … 225 км/год для значення несучої частоти 2,4 ГГц. У розробленій моделі завмирання вважаємо незалежними, тобто передбачено рознесення каналів на декілька довжин радіохвилі, що дало можливість отримати максимальний енергетичний виграш (ЕВ) від рознесення. Вибір конфігурацій MIMO 2×1 та 2×2 гарантує мінімальні масо-габаритні показники мобільних станцій при забезпеченні необхідного рівня декореляції антен, що важливо для оперативного та ефективного виконання завдань у сучасних СБЗСП. Результати імітаційного моделювання наведено у вигляді залежності величини ймовірності бітової помилки $P_{пом}$ від SNR.

Отримані результати показують, що методи STBC/SFBC-OFDM-IM дозволяють підвищити достовірність передачі інформації за рахунок отриманого ЕВ до 8 дБ при ймовірності бітової помилки $P_{пом} = 10^{-5}$ та одночасно підвищити СЕ до 20% у порівнянні з класичними STBC/SFBC-OFDM. Додатково покращити показники ЕЕ та СЕ таких схем STBC/SFBC-OFDM-IM можливо завдяки концепції дворежимної (Dual Mode) індексної модуляції піднесучих з базовими для СБЗСП удосконаленими ансамблями BPSK, QPSK та 16-QAM. Новаторська ідея DM-OFDM-IM полягає у відсутності (на відміну від OFDM-IM) вимкнених з передачі піднесучих, з отриманням індексних біт завдяки забезпеченню можливості надійного визначення потенційно диференційовних пар ансамблів сигналів. Використання таких методів дозволяє отримати ЕВ до 4 дБ при ймовірності бітової помилки $P_{пом} = 10^{-4}$ та одночасно підвищити СЕ до 17% у порівнянні з однорежимними STBC/SFBC-OFDM-IM. Розробка універсального ефективного методу просторового кодування з DM-OFDM-IM об'єктивно ускладнюється протиріччям між впливом часової та частотної селективності на структурно-параметричну оптимізацію багатоантенних систем з OFDM. Саме тому, в частотно-селективних каналах (ПС та ВС) з низьким рівнем нестаціонарності ($F_{\text{Д}} < 0{,}01$) слід використовувати метод просторово-часового блочного кодування з DM-OFDM-IM. Для забезпечення якісного зв'язку з високодинамічними наземними об'єктами та літальними апаратами різного призначення в каналах ПС з переважаючою нестаціонарністю ($F_{\text{Д}} \geq 0{,}05$) рекомендовано застосовувати метод просторово-частотного блочного кодування з DM-OFDM-IM, що є потенційно стійким до неінваріантних у часі статистичних параметрів каналу. Подальше підвищення СЕ методу SFBC-DM-OFDM-IM можливе за рахунок збільшення кількості індексних біт шляхом забезпечення інваріантності даного методу до нерівномірності амплітудно-частотної характеристики (АЧХ) та нелінійності фазо-частотної характеристики (ФЧХ) для будь-якої комбінації пар піднесучих у субблоці.

Слід зазначити, що СКК з одно- та дворежимною індексною модуляцією OFDM-IM є найбільш результативними при невеликих розмірах субблоків та ансамблів сигналів. Зазначені методи можуть бути продуктивно використані у технологіях безпроводового зв'язку нового покоління, а також у сучасних СБЗСП, що потребують реалізації об'ємних мультимедійних додатків зі СЕ до 4,25 біт/с/Гц у складній завадовій обстановці. Це дасть потенційну можливість покращити ефективність системи зв'язку між військовими підрозділами та центрами стратегічного і тактичного управління, що в умовах сучасної гібридної війни безпосередньо визначає боєздатність армії вцілому, тим самим підвищуючи інформаційну безпеку держави.

к.ф.-м.н. Сорокатий М.І. (НАСВ)
к.т.н. Петрученко О.С. (НАСВ)
к.е.н. Білаш О.В. (НАСВ)

СПЕЦИФІКА ВИКЛАДАННЯ ВИЩОЇ МАТЕМАТИКИ У ВВНЗ

Актуальність. Низка законодавчих документів стосовно вищої освіти підкреслюють про недопущення зниження якості освіти та падіння рівня знань загалом. Розуміння того, що якісна освіта – це один із головних факторів розвитку держави, який спонукає шукати нові шляхи та підходи до підготовки висококваліфікованих військових спеціалістів, офіцерів-патріотів.

Мета. Постійні зміни, які відбуваються в освітньому процесі зумовлюють необхідність впровадження нового підходу до викладання навчальних дисциплін, який повинен бути спрямований на курсант і з врахуванням сучасних тенденцій. Передовсім ці зміни повинні полягати в організації нестандартних лекційних, практичних, лабораторних занять, індивідуалізації навчання, застосування нової системи контролю знань, навчально-методичної літератури нового рівня. Все це зумовлює необхідність розробки нових підходів до викладання вищої математики.

Основні положення. Варто зазначити, що кожний курсант – це особистість, тому немає двох однакових курсантів. В зв'язку з цим і підходи до їхнього навчання повинні бути різними. В ідеалі – це індивідуальне навчання. При проведенні практичних занять викладач старається максимально індивідуалізувати завдання, які виконуються курсантами. При цьому у них виробляється впевненість, що навчання дійсно відбувається. Індивідуальний підхід дозволяє розглядати викладача і курсанта як партнерів, які разом закладають основи знань.

Альтернативою індивідуального підходу є кооперативне навчання. На нашу думку, поєднання індивідуального підходу з кооперативним для наших курсантів є найбільш ефективним. Складовими цього підходу є:

– історичний підхід у викладанні навчального матеріалу з відзначенням ролі видатних, зокрема українських вчених;

– професійна спрямованість дисципліни;

– методичне забезпечення;

– використання Інтернету та навчальних фільмів.

З історичних джерел відомо про ключову роль математики і природничих наук у розвитку військової техніки. До перших із них можна віднести відкриття знаменитого вченого Архімеда в обороні рідних Сіракуз (на Сицилії) від нападу римської армії в далекому третьому столітті до нової ери. Метальні машини, угнуті дзеркала та інші придумані вченим пристрої допомагали протягом довгого часу вистояти сіракузцям супроти могутнього римського війська. Подібних прикладів відомо багато у всі епохи. Згадаємо принагідно про Архипа Люльку - уродженця с. Саварка нині Богуславського району Київської області. Створені ним двигуни стоять на багатьох сучасних військових літаках. Курсантам буде цікаво взнати, що видатний військовий діяч, артилерист-винахідник, творець бойових ракет Олександр Дмитрович Засядько, є українцем за походженням, родом з Полтавщини. Він порушив питання про застосування ракет вітчизняної конструкції у майбутніх бойових діях з турецькими військами, в результаті чого була створена спеціальна ракетна рота, оснащена бойовими ракетами і пусковими станками для ведення залпового вогню. Варто відзначити українських математиків, які здійснили вагомий вклад у розвиток військової науки: Михайла Остроградського, Георгія Вороного, Михайла Кравчука, Віктора Глушкова та багатьох інших. Такі відомості формують самоповагу і патріотизм курсантів, відчуття їхньої вагомості у світі та необхідність захищати своє становище і свою країну.

Підготовка кваліфікованих фахівців у вищих військових навчальних закладах України в останні роки зазнає суттєвих змін, які пов'язані з появою нових та вдосконаленням існуючих спеціальностей, інтеграцією знань із суміжних галузей діяльності людини,

впровадженням і використанням сучасних комп'ютерних і телекомунікаційних технологій. Професійна підготовка вимагає узгодженості знань, які торкаються військової справи, техніки та сучасних технологій. Це, передусім, передбачає науково обґрунтоване проектування навчальних планів і програм, забезпечення їх раціональної структури, дидактично доцільного поєднання загальноосвітніх, загальнопрофесійних, професійно орієнтованих (спеціальних) предметів, узгодженості програм взаємопов'язаних дисциплін, професійної спрямованості навчання.

Головними напрямами реалізації принципу професійної спрямованості під час вивчення природничо-математичних дисциплін у ВВНЗ є:

– історичний підхід у викладанні навчального матеріалу з відзначенням ролі видатних, зокрема українських вчених;

– вивчення основ наук з обов'язковою конкретизацією законів, правил, формул тощо, професійними відомостями;

– систематичне розв'язання задач і завдань із змістом військового спрямування;

– побудова навчального процесу таким чином, щоб структура пізнавальної діяльності курсантів відповідала структурі їхньої майбутньої професійної діяльності.

Здійснюючи професійну спрямованість, важливо пам'ятати, що зміст кожного загальноосвітнього предмета – це основи відповідної науки, і тому в головному він має бути підпорядкований внутрішній логіці конкретної науки, а не утилітарним запитам професійної підготовки. Професійна спрямованість забезпечується також більш глибоким вивченням законів і теорій, покладених в основу технологічних процесів, із якими курсанти ознайомлюються під час розв'язання задач із виробничим змістом і проведення практичних робіт, пов'язаних із майбутнього професійною діяльністю. Врахування взаємозв'язку загальної і професійної освіти сприяє цілеспрямованому, систематичному, поглибленому вивченню взаємопов'язаних понять природничо – математичних предметів і дисциплін професійно – теоретичного циклу, посилює функції природничо – математичних предметів як теоретичної базової основи професійного навчання.

Сучасні педагоги вважають, що слід замінити традиційну „накопичувальну" освіту, яку вони називають „банківською", на освіту „проблемно‑визначальну". Кафедра інженерної механіки (ОТІВ) факультету підготовки спеціалістів бойового (оперативного) забезпечення Національної академії імені гетьмана Петра Сагайдачного проводить підготовку курсантів із природничо-наукових дисциплін та дисциплін військово-професійної спрямованості. Кожна із дисциплін, зокрема, вища математика, забезпечена навчально-методичними посібниками, які розроблялися викладачами кафедри. Впроваджуючи „проблемно‑визначальний" підхід до надання освіти кафедрою запропоновано інтенсифіковано проводити практичні заняття таким чином, щоб максимально стимулювати курсантів до самостійного виконання завдань. Практичне заняття проводиться у такій послідовності:

крок 1: оголошення результатів попереднього поточного контролю;

крок 2: поточний контроль;

крок 3: повторення вивченого, роз'яснення викладачем нового матеріалу;

крок 4: робота на індивідуальними завданнями під контролем викладача;

крок 5: оцінка роботи курсантів, feedback, проведення підсумків;

крок 6: видача завдань для самопідготовки.

Застосовувати знання, отримані при вивченні навчальних дисциплін курсанти можуть при написанні конкурсних робіт під час навчання в гуртках науковця початківця та ВНТК.

Висновок. Отже, методика проведення практичних занять відіграє важливу роль у покращенні засвоєння матеріалу військовими фахівцями у ВВНЗ, а впровадження у навчальний процес системи багаторівневого навчання та контролю знань курсантів із різним рівнем базових знань спонукає їх до активної роботи під час практичних занять та самостійної підготовки, дозволяє систематично перевіряти рівень засвоєння лекційного і практичного матеріалу.

Степаненко Є.О. (ВІТІ)

ОЦІНКА ЕФЕКТИВНОСТІ МЕТОДИК УПРАВЛІННЯ ТОПОЛОГІЄЮ НАЗЕМНО-ПОВІТРЯНИХ РАДІОМЕРЕЖ

В процесі побудови математичних моделей функціонування наземно-повітряних радіомереж (НПР) [1] доводиться вирішувати компроміс між повнотою опису мережі і складністю адекватних їй моделей.

Тому при математичному моделюванні НПР найбільш доцільно суміщати аналітичні та імітаційні моделі.

Методика управління топологією, яка входить до підсистеми управління топологією системи управління, безпосередньо буде впливати ефективність функціонування системи управління в цілому [2]. Тому запропонована класифікація показників оцінки ефективності методики управління топологією на функціонування НПР, яка наведена на рис. 1.

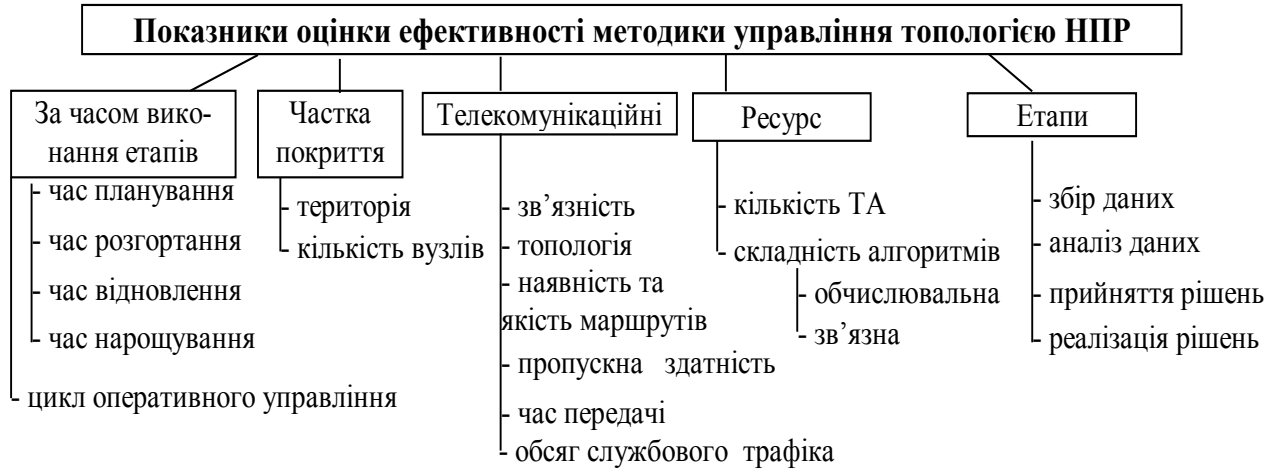


Рис. 1. Класифікація показників оцінки ефективності управління

Методика управління топологією НПР буде використовуватися в спеціальному програмному забезпеченні системи управління мережею на різних етапах її функціонування (планування, розгортання, відновлення, нарощування, оперативного управління) для розрахунку положень телекомунікаційних аероплатформ (ТА) у просторі та вибору режимів роботи радіо-засобів [2]. Часові інтервали на реалізацію даних етапів повинні бути не більше заданих, тобто час планування $t_{пл} \le t_{плзад}$, час розгортання $t_{роз} \le t_{роззад}$, час відновлення (нарощування) $t_{від} \le t_{відзад}$ мережі повинні бути не більше заданих (директивних).

Тобто час отримання рішення з топології НПМ повинен задовольняти часові вимоги з реалізації цих етапів.

Ефективність оперативного управління може визначатися:

1. Часом циклу управління $T_ц$

$$T_ц \to T_{зб} + T_{ан} + T_{пр} + T_{рр} \to \min,$$

де $T_{зб}$ – час збору даних про стан мережі, $T_{ан}$ – час, який витрачається на аналіз стану мережі, $T_{пр}$ – час прийняття рішень з управління (визначається складністю математичних моделей, розмірністю задач та апаратними обчислювальними можливостями), $T_{рр}$ – час реалізації рішень (визначається розмірами району дислокації наземних вузлів, ТА, технічними характеристиками ТА).

2. Якістю прийнятих рішень центром управління мережею, системами управлінь ТА, системами управління наземними вузлами.

Якість в загальному оцінюється ступенем досягнення мети управління на множині

показників функціонування мережі, витраченими ресурсами, обсягом службової інформації $V_{ст}$, що витрачається на її реалізацію.

Тут існує класичне протиріччя проблеми управління мережею.

Чим більше збираємо службової інформації про стан мережі (збільшуємо обсяг службового трафіка), тим кращі рішення приймаємо (за умови адекватності моделей управління мережею). І навпаки.

Чим менше збираємо службової інформації про стан мережі (зменшуємо обсяг службового трафіка), тим менш якісне рішення приймаємо.

Показниками якості покриття є ступінь покриття заданої території або відсоток покритих вузлів. Для підсистеми телекомунікацій системи управління ТА основними показниками оцінки ефективності є: зв'язність, пропускна здатність, затримка передачі, варіації затримки передачі даних (джиттер), ймовірність помилок тощо.

Розглянемо деякі з них більш детально.

Зв'язність може визначатись на канальному рівні наявністю або відсутністю радіоканалу передачі, на мережевому – кількістю (відсотком) незв'язних підмереж.

Поняття k-зв'язність визначає наявність k-маршрутів передачі тощо.

Мережа вважається працездатною до тих пір, поки існує зв'язна топологія та маршрути доставки даних.

Необхідно відзначити, що потенційно можливі маршрути передачі визначаються попередньо побудованою системою управління топологією мережі.

Якість кожного з маршрутів всієї множини маршрутів характеризується своїми параметрами: пропускна здатність, затримка передачі, час існування, час побудови та ін.

Крім цього якість маршрутів та їх наявність визначається поточною топологією мережі, яку можна оцінити наступними показниками: час побудови, ступінь зв'язності вузлів, діаметр мережі, щільність розміщення вузлів, потужності передач вузлів, величина енерговитрат вузлів і т.п.

Параметри якості обслуговування залежать від типу трафіка.

Наприклад, для мультимедійних додатків повинні бути гарантовані вимоги: з пропускної здатності, затримки, джитера і втрат.

Тобто мережа (підмережа) повинна забезпечити пропускну здатність $S_м$ не нижче заданої $S_м > S_{зад}$, (визначається додатком) в межах заданого проміжку часу.

У свою чергу пропускна здатність мережі $S_м$ визначається як сума пропускних спроможностей її інформаційних напрямів. Пропускна здатність напряму s_j дорівнює сумі пропускних спроможностей маршрутів в цьому напряму, а пропускна здатність маршруту дорівнює мінімальній пропускній здатності l-го каналу, що входить в цей маршрут m:

$$S_м = \sum_{j=1}^{J} s_{j,}\ \ s_j = \sum_{m=1}^{M} s_m,\ \ s_m = \min_{i \in m}\{k_l\}.$$

Гарантований час передачі даних – гарантія того, що доставка даних від відправника до адресата виконується в строго певний інтервал часу $t_{пер} \le t_{зад}$.

Гарантія варіації затримки – свідоцтво того, що затримки, що вносяться компонентами системи уздовж всього маршруту переміщення даних, знаходяться в строго визначених межах.

Гарантія втрат – умова, при виконанні якої втрати даних не перевищують задану додатком частку пакетів в процесі їх передачі від джерела до споживача.

Важливими показниками є кількість ресурсів, які витрачаються на процес управління НПМ: кількість ТА, складність алгоритмів – обчислювальна та зв'язна (обсяг службового трафіка та час, який витрачається на реалізацію алгоритму).

Кожний з етапів управління (збір, аналіз, прийняття та реалізація рішень) крім часових показників може оцінюватися низкою додаткових.

Наприклад, збір даних із сенсорних вузлів – кількість, період та тип збору даних; аналіз – кількість параметрів аналізу, кількість моделей аналізу тощо.

Для оцінки ефективності методик було проведено моделювання за допомогою систем моделювання MATLAB та ns-2. Система MATLAB використовувалась для розрахунку положення ТА у просторі (реалізація алгоритмів кластеризації), розрахунку положення ТА в зоні обслуговування наземних вузлів (реалізація моделі позиціонування ТА з метою оптимізації пропускної здатності наземних вузлів зони обслуговування), розрахунку положення ТА в повітряній мережі (реалізація моделі позиціонування ТА для оптимізації пропускної здатності повітряної мережі).

Отримані рішення (положення ТА) є вхідними даними для системи моделювання ns-2.

В імітаційній моделі відповідно до моделі OSI визначені фізичний, канальний, мережевий, транспортний та прикладний рівні. На фізичному та канальному рівнях використовується протокол IEEE 802.11, який визначає потужність передавача, технології завадостійкого кодування, допустиму швидкість передачі тощо.

Мережі FANET можуть розглядатися як різновид мережі MANET та VANET, однак вони мають ряд своїх особливостей:

рівень мобільності значно вищий, тому можлива швидка зміна топології;

вхідний трафік розподіляється за наступними напрямами: НВ-ТА і далі ТА-НВ своєї зони, ТА-ТА-НВ іншої зони або ТА-ТА-вузол стаціонарної компоненти;

відстань між ТА значно більша чим між наземними вузлами.

В моделі визначено:

фізичний та канальний рівні, які описуються в мережевому дискретно-подійному симуляторі YAS, режим – ad-hoc, версія стандарту 802.11, частотний діапазон;

ширина смуги кожного каналу (МГц); потужність передавача наземного вузла – однакова для всіх наземних вузлів; потужність передавача ТА – однакова для всіх ТА; потужність шуму на вході приймача однакова для всіх вузлів; поріг енергії для виявлення сигналу (-100 дБ); модель загасань у вільному просторі.

На мережевому рівні працює протокол IPv4, використовується протокол маршрутизації AODV. На транспортному рівні використовується протокол TCP або UDP.

Вузли наземної мережі розташовані випадковим чином на певній площині.

Моделі переміщення вузлів – модель групового переміщення.

У відповідності з постановкою задачі, дослідження вхідними даними імітаційної моделі виступають характеристики НПР та методики управління топологією наземних мереж з ТА.

Характеристиками мережі є: кількість вузлів та їх характеристики, топологія та динаміка її зміни мережі. Кожен вузол в мережі в ході його моделювання може бути описаний сукупністю параметрів, які різносторонньо відображають процес його функціонування. Вузол наземної мережі (НМ) може бути описаний з різних позицій: координати, характеристики радіозасобів, вхідне навантаження кожного вузла визначається вимогами бою та прийнятою системою управління військами.

Певний вузол може генерувати повідомлення різного розміру, пріоритету, типу (дані, відео), які визначають різні вимоги до якості обслуговування.

Функціонування ТА задається наступною множиною параметрів: швидкість, напрямок та висота польоту, граничний час польоту, параметри радіообладнання тощо.

Так, з точки зору еталонної моделі взаємодії відкритих систем, вузол може моделюватися на фізичному, канальному, мережевому або транспортному рівнях.

На фізичному рівні параметрами моделювання є швидкість передачі, тип модуляції, параметри антени, вихідна потужність передавача та ін. Канальний рівень визначає спосіб розділення каналу (частотний, часовий), протокол доступу до каналу (випадковий, з контролем несучої і т.д.). На мережевому рівні визначається метод маршрутизації. На транспортному рівні приймаються до уваги протоколи обміну інформацією за напрямом (кількість повторних передач, час очікування квитанції тощо) та управління навантаженням.

На прикладному – розроблені методики управління топологією.

План проведення досліджень складається з наступних кроків.

1. Оцінка ефективності запропонованої методики побудови зв'язної топології наземних радіомереж із застосуванням телекомунікаційних аероплатформ за показниками:

зв'язність – залежність частки (в %) зв'язних підмереж при використанні різної кількості ТА; залежність коефіцієнту часу зв'язності та коефіцієнту стабільності маршрутів від рівня мобільності наземних вузлів;

залежність зв'язності від тривалості циклу управління методики;

пропускна здатність зони обслуговування ТА – залежність від приросту пропускної здатності наземних мереж зони обслуговування ТА в залежності від рівня трафіка та розташування наземних вузлів;

обчислювальна складність алгоритму реалізації методики.

2. Оцінка ефективності методики управління топологією наземних мереж із забезпечення заданої якості інформаційного обміну за показниками пропускної здатності, часу передачі даних, обчислювальна складність алгоритму реалізації методики.

Проведені дослідження ефективності запропонованих методик управління топологією наземних мереж при різних вихідних даних: розмірність мережі, кількість ТА, кількість наземних вузлів в кластері, різні варіанти розміщення наземних вузлів, різні рівні навантаження тощо. Результати моделювання продемонстрували, що запропонована методика побудови зв'язної топології НМ з використанням ТА:

потребує до 25 % меншої кількості ТА, ніж при використанні відомих алгоритмів розміщення ТА, обчислювальна складність алгоритмів FOREL та k–середніх – $O(N^2)$;

надає можливість збільшити пропускну здатності зони обслуговування ТА до 15 – 30 % в залежності від кількості наземних вузлів в зоні та варіантів їх розміщення.

Обчислювальна складність моделі позиціонування незначна та дорівнює $O(n_T n^2)$, де n_T – кількість точок в зоні переміщення ТА, n – кількість вузлів в зоні.

Це дозволяє використовувати методику в системі управління ТА для отримання рішення з її положення в реальному масштабі часу.

Проведена оцінка ефективності методики управління топологією наземних радіомереж з використанням телекомунікаційних аероплатформ для забезпечення заданої якості інформаційного обміну. Результати імітаційного моделювання показали, що застосування методики дозволяє збільшити пропускну здатність наземної мережі (в середньому до 30 %); зменшити середній час затримки передачі повідомлень при незначному об'ємі службового трафіка (при централізованому управлінні витрачається $O(2N)$ повідомлень, де N – кількість вузлів мережі, при децентралізованому – $O(2n_{суc})$, де $n_{суc}$ – кількість сусідніх ТА.

Отримання рішення здійснюється в масштабі реального часу.

Таким чином, застосування методики дозволяє покращити показники функціонування наземної мережі в певних маршрутах, напрямах, зонах та всієї наземної мережі за рахунок створення додаткових маршрутів передачі через повітряну мережу та перерозподілу частки трафіка з наземної мережі на повітряну.

Наприклад, застосування ТА дозволяє в декілька разів скоротити кількість ретрансляційних ділянок в маршрутах передачі (в залежності від розмірності мережі ця величина зменшується в 2 – 4 рази), тим самим збільшувати пропускну здатність мережі та зменшувати час передачі. Реалізація запропонованих методик управління топологією наземних вузлів з використанням ТА в спеціалізоване програмне забезпечення системи управління НПР дозволяє отримати зв'язні топології наземних радіомереж та значно покращити показники функціонування наземної мережі.

ЛІТЕРАТУРА

1. Романюк В.А., Степаненко Є.О., Панченко І.В., Восколович О.І. Літаючі самоорганізуючі радіомережі. Збірник наукових праць ВІТІ. 2017. №1. С. 104 – 114.

2. Романюк В.А., Степаненко Є.О. Методика управління топологією наземно-повітряних радіомереж військового призначення. Збірник наукових праць ВІТІ. 2018. № 4. С. 92 – 103.

к. пед. н. Ступак Д. Є. (ЖВІ)

МЕТОДИКА ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ ГАРАНТУВАННЯ ЯКОСТІ ВИЩОЇ ВІЙСЬКОВОЇ ОСВІТИ

Актуальність. Підготовка військових фахівців з вищою освітою на сучасному етапі розвитку вищої школи вимагає вдосконалення освітнього процесу, підвищення його ефективності на засадах компетентнісного підходу, оскільки теоретичні знання та практичні уміння, набуті курсантами під час освітньої та професійної підготовки у вищому військовому навчальному закладі (ВВНЗ), закладають основу ефективної реалізації ними фахових компенцій та успішної майбутньої професійної діяльності.

Метою досліджень є розробка методики оцінювання ефективності функціонування системи гарантування якості вищої військової освіти у ВВНЗ, ВНП ЗВО (військово-навчальних підрозділах закладів вищої освіти) МО України та пропозицій щодо внесення змін у керівні документи стосовно запровадження системи гарантування якості вищої військової освіти з урахуванням досягнень вітчизняного досвіду та досвіду держав-членів НАТО.

Основні положення. Відповідно ст. 1 Закону України „Про вищу освіту” результат навчання – сукупність знань, умінь, навичок, інших компетентностей, набутих особою у процесі навчання за певною освітньо-професійною, освітньо-науковою програмою, які можна ідентифікувати, кількісно оцінити та виміряти.

Кількісна та якісна оцінки ефективності функціонування системи забезпечення якістю ВВНЗ утруднені через не врахування особливостей їх функціонування.

Зельницький А. наголошує, що „забезпечення”, в контексті якості освіти, необхідно розглядати як процес, а „гарантія” – як результат процесу щодо досягнення мети освітньої діяльності.

Гарантія якості вищої військової освіти – це порука та відповідальність ВВНЗ щодо виконання державного замовлення з підготовки слухачів (курсантів) зі ступенем сформованості визначених компетентностей в кожного з них не нижче встановленого рівня.

Відповідно до міжнародного стандарту, щодо забезпечення якості в Європейському просторі вищої освіти (ESG-2015) забезпечення якості освіти ґрунтуються на таких чотирьох принципах у Європейському просторі вищої освіти (European Higher Education Area - EHEA):

1. Заклади вищої освіти несуть первинну відповідальність за якість вищої освіти, що надається.
2. Забезпечення якості відповідає різноманітності систем вищої освіти, закладів вищої освіти, програм і студентів.
3. Забезпечення якості сприяє розвитку культури якості.
4. Забезпечення якості враховує потреби та очікування студентів, усіх інших стейкхолдерів та суспільства.

За результатами вивчення наукової літератури та аналізу досвіду ВВНЗ нами встановлено, що основними індикаторами, що безпосередньо визначають якість вищої освіти (ефективність організації освітнього процесу) є сукупність характеристик ВВНЗ, а саме: мотиваційний ресурс; інформаційний ресурс; навчально-методичний ресурс; науково-інноваційний ресурс; матеріально-технічний ресурс; адміністративно-управлінський ресурс; морально-психологічний клімат у колективі; нормативно-правова база тощо.

Комплексна оцінка ефективності функціонування ВВНЗ дозволяє отримати необхідні дані про результати їх діяльності, можливість розрахувати показник ефективності використання ресурсів, а також, запропонувати рекомендації щодо підвищення ефективності функціонування.

Запропонована методика оцінки здійснюється в три етапи:

І. Вибір та визначення показників певного ресурсу освітньої діяльності ВВНЗ, ВНП ЗВО МО України.

ІІ. Розрахунок інтегральних показників освітньої діяльності окремого ВВНЗ, ВНП ЗВО МО України.

ІІІ. Розрахунок комплексного показника та аналіз результатів діяльності ВВНЗ, ВНП ЗВО МО України

Перший та другій етап методики включає вибір та розрахунок показників, що відображають результати діяльності окремих ВВНЗ, ВНП ЗВО МО України. Він дозволяє оцінити ступінь досягнення основної мети ВВНЗ – надання освітніх послуг, що забезпечує готовність випускників до виконання завдань за призначенням відповідно до європейських та євроатлантичних стандартів.

Третій етап передбачає розрахунок комплексного показника результатів діяльності ВВНЗ, ВНП ЗВО МО України, з метою проведення аналізу ефективності системи гарантування якості вищої військової освіти в Україні.

Для вимірювання та визначення рівня необхідних ресурсів для ефективної організації освітнього процесу ВВНЗ, ВНП ЗВО МО України пропонується:

– визначати кількісний рівень окремого показника індикатора за методом зважених сум, коли кожен визначальний показник має свою вагомість;

– для визначення якісного рівня окремого показника індикатора використати перетворення за шкалою Харрінгтона з певною модифікацією, яке дозволяє перевести кількісне значення (наприклад, частку або відсоток) у якісне значення.

Для визначення кількісного рівня необхідних ресурсів для ефективної організації освітнього процесу ми пропонуємо використовувати лише дві шкали: дихотомічну (так/ні=1/0), яка свідчить про наявність/відсутність певної характеристики та метричну (кількісну).

На нашу думку, застосування даних шкал знижує суб’єктивність в оцінюванні.

Порядок оцінювання ефективність організації освітнього процесу на основі даного методу полягає у перевірці конкретного процесу (індикаторів) із визначенням ступеня виконання відповідних критеріїв (показників) за заздалегідь встановленою деталізованою (уніфікованою) шкалою.

Отже, за кожним індикатором можна визначити рівень внутрішнього забезпечення якості. Це дозволяє виявити «вузькі місця» ВВНЗ в організації освітньої діяльності з позицій забезпечення (гарантування) якості освіти, а також сприяє формуванню необхідних управлінських впливів для подальшого розвитку системи вищої військової освіти в Україні. Аналіз результатів в динаміці дозволить виявити тенденції у функціонуванні системи внутрішнього забезпечення (гарантування) якості та своєчасно відреагувати на недоліки в її організації.

Основною перевагою пропонованої методики є те, що вона дає можливість отримати підсумковий результуючий показник. Практичне значення цієї методики, на наш погляд, посилюється нині в процесі реформування системи вищої військової освіти, а саме в підвищення якості підготовки висококваліфікованих фахівців відповідного рівня та спеціальності, конкурентоспроможних, компетентних, відповідальних, морально вихованих, які вільно володіють своєю професією, орієнтуються в суміжних сферах діяльності, здатних до ефективної професійної діяльності на рівні світових стандартів, готових до постійного професійного зростання, соціальної та професійної мобільності.

Здійснене дослідження не вичерпує усіх аспектів, що пов’язані з проблемою ефективності функціонування системи гарантування якості вищої військової освіти.

Висновок. Таким чином, оцінка, що визначається за допомогою наведеної методики, характеризує спроможність системи забезпечення якості вищої військової освіти відповідати своєму призначенню – забезпечувати стабільне виконання всіх встановлених вимог до діяльності ВВНЗ, що впливає на якість навчання (виконання зобов’язань перед замовниками), а також дає можливість відстежувати зміни, аналізувати тенденції розвитку системи управління якістю та своєчасно вживати коригувальні та запобіжні дії, зменшувати ризики та постійно удосконалювати освітню діяльність.

д.п.н. Сусь Б. (ВІТІ)
к.т.н. Грохольський Я. (ВІТІ)

ФІЗИЧНИЙ ЗМІСТ ПОНЯТТЯ “СТРУМ ЗМІЩЕННЯ”

Актуальність. Традиційно електричний струм розглядається, як рух зарядів по всьому замкненому електричному колу, і ознакою струму є магнітне поле. Однак таке визначення справедливе тільки для постійного струму у сталому режимі, коли коло не розірване конденсатором. При наявності конденсатора заряди не можуть рухатись по всьому колу, тому першопричиною змінного струму є електричне поле, яке виникає одночасно із змінним магнітним полем і на ділянці провідника приводить у рух заряди. Питання полягає у поєднанні фізичних процесів, які пов’язані з перенесенням електричних зарядів.

Аналіз проблеми. Традиційно електричний струм розглядається як рух електричних зарядів в електричному колі під дією електричного поля, яке створюється джерелом струму з електрорушійною силою ε. Сила струму дорівнює кількості заряду q, який проходить через поперечний переріз провідника за одиницю часу: $I = q/t$. У провідниках (металах) носіями зарядів є електрони як елементарні частинки.

Ознакою струму є магнітне поле навколо провідника, по якому тече струм, що підтверджується практично. Уявлення про струм сформувались історично і вони відображають процеси, що пов’язані з протіканням струму в електричному колі. Однак ці уявлення є в певній мірі умовними, на що звернув увагу Максвелл, створюючи теорію електромагнітних хвиль. Якщо в електричному колі знаходиться конденсатор C, то фактично існує розрив електричного кола і постійний струм протікати не може, тому що зарядів у проміжку між пластинами конденсатора нема, є тільки постійне електричне поле $\vec{E}$ між ними, отже, їх руху бути не може, гальванометр G показує 0 (рис.1а).

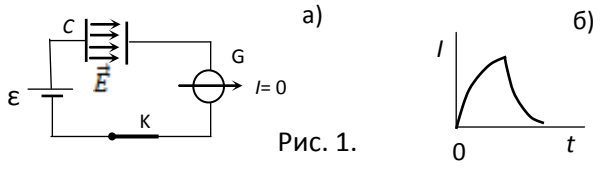


Рис. 1.

Однак у колі з конденсатором може протікати **змінний** електричний струм, що й спостерігається при замиканні кола із джерелом постійної напруги (перехідний процес). У момент замикання кола гальванометр показує зростання струму з подальшим спаданням його до нуля (рис. 1б). Максвелл такий струм умовно назвав **струмом зміщення.**

Якщо джерело струму генерує змінний струм, то такий струм, як відомо, завжди через конденсатор протікає, і його величина залежить від опору конденсатора, який, у свою чергу, залежить від ємності конденсатора. В обох випадках виникає необхідність у поясненні, чому по всьому замкненому колу протікає струм, але заряди між пластинами конденсатора не переміщуються. Хоча, згідно стандартних, широко використовуваних визначень, струм – це напрямлений рух зарядів. Як видно, виникає несумісність між визначенням струму, як напрямленого руху зарядів, і твердженням, що струм протікає по всьому колу, хоча між пластинами конденсатора заряди не рухаються. Струм зміщення на ділянці конденсатора, де нема зарядів, Максвелл пов’язав зі **змінним** електричним полем, що виникає в момент замикання кола. При замиканні кола до однієї з пластинок конденсатора відбувається притік зарядів від джерела е.р.с., а від другої – відтік.

Тобто, відбувається зміна зарядів на пластинах і відповідна зміна електричного поля в проміжку між пластинами. Густина струму зміщення $j_{зм} = dD/dt$, де $D = \varepsilon \varepsilon_o E$ – індукція, а E – напруженість електричного поля. Таким чином, формально струм протікає по всьому замкненому колу, але на ділянці конденсатора струм – це вже не є рух зарядів. Тому Максвелл умовно назвав цей струм „струмом зміщення”. Виходить, що традиційне

означення струму по суті не відображає механізму протікання струму. Тому виникає потреба конкретизувати фізичний зміст поняття „електричний струм” і механізм його протікання.

Отже, при замиканні кола з конденсатором з’являється електричний струм, який на ділянці провідника розглядається як напрямлений рух зарядів. Традиційно вважається, що ознакою електричного струму є магнітне поле, яке виникає навколо нього. Тому, коли струм тече по **провіднику**, то є реальне переміщення зарядів (електронів) і існує зв’язок між напрямленим рухом зарядів і магнітним полем навколо провідника (рис.2).

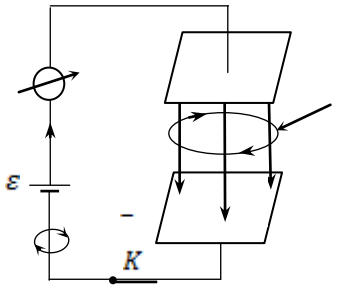


Рис. 2.

Однак на ділянці конденсатора електронів нема і нема їх руху. Але магнітне поле на ділянці конденсатора існує.

Треба додати, що антена у радіозасобах випромінювання – це специфічно розкритий конденсатор стосовно землі, який забезпечує випромінювання електромагнітних хвиль. Стан цих хвиль у процесі їх поширення розглянутий в. Логічно зробити висновок, що не струм як напрямлений рух зарядів створює магнітне поле, а швидше навпаки – заряди рухаються тому, що є магнітне поле, оскільки воно існує на всіх ділянках кола.

Зауважимо, що йдеться про змінне магнітне поле, яке виникає в момент замикання кола. Як бачимо, існує неузгодженість в логіці міркувань – що ж є первинним у визначенні поняття струму як напрямленого руху зарядів?

Струм, який створює магнітне поле, яке є ознакою струму, чи магнітне поле якимось чином є причиною руху зарядів? Відповідь знаходиться у рівняннях Максвелла, з яких випливає, що **змінне магнітне поле існує одночасно зі змінним електричним полем.** А це означає, що при замиканні кола відбувається зростання електричного поля не тільки між пластинами конденсатора, але також на проміжку провідника.

Оскільки на ділянці провідника є заряди, то вони й приходять у рух під дією електричного поля і створюють електричний струм провідності у його традиційному тлумаченні. На проміжку ж між пластинами конденсатора руху зарядів нема і струму провідності також нема, але є змінне електричне поле $\boldsymbol{E}$ і змінне магнітне поле $\boldsymbol{H}$. Таким чином, насправді йдеться про виникнення так званого електромагнітного поля як одночасного зростання чи спадання напруженостей електричного і магнітного полів, що й випливає з рівнянь Максвелла. Так що не рух зарядів є першопричиною магнітного поля навколо струму, а заряди в провіднику рухаються і створюють струм завдяки електричному полю $\boldsymbol{E}$, що виникає разом з магнітним полем при замиканні електричного кола.

Зміна електричного і магнітного поля являє собою електромагнітну хвилю, яка поширюється в усі сторони від провідника, що реалізується в антені передавального радіотехнічного пристрою. Цей взаємозв’язок полів існує не тільки у процесі самостійного розповсюдження електромагнітної хвилі у просторі, а й у процесі її початкового формування в електричних колах технічних радіосистем.

Висновок. Традиційно електричний струм розглядається як рух зарядів по всьому замкненому колу і ознакою струму є магнітне поле.

Однак таке визначення справедливе тільки для постійного струму. При змінному струмі першопричиною є не струм, а змінне електричне поле, яке виникає разом зі змінним магнітним, і на ділянці провідника приводить у рух заряди.

Тарара В.М. (ВІТІ)
Нерознак Є.І. (ВІТІ)

РЕАЛІЗАЦІЯ ВІДДАЛЕНОГО ДОСТУПУ ДО КОМП'ЮТЕРНИХ МЕРЕЖ ПУНКТІВ УПРАВЛІННЯ ЗС УКРАЇНИ

Актуальність даної роботи пов'язана з тим, що постійне збільшення кількості операторів автоматизованих робочих місць пунктів управління, які знаходяться на значних географічних відстанях один від одного, призводить до необхідності використання технології віддаленого доступу. Однак, це потребує вирішення питання захисту службової інформації, яка передається відкритими каналами зв'язку через мережі загального користування.

Метою зазначеного дослідження є реалізація віддаленого доступу до мереж та автоматизованих робочих місць пунктів управління з використанням захищених протоколів для здійснення управління та адміністрування територіально-розподіленими мережами в реальному часі.

Метод віддаленого доступу може відрізнятися типом служб, які підтримуються для віддаленого клієнта. Найчастіше використовується віддалений доступ до мережевого та серверного обладнання, автоматизованих робочих місць, файлів, баз даних, тощо.

Крім можливості локального доступу до управління зазначеними об'єктами, віддалений доступ до них, з урахуванням специфіки використання у військовій сфері, повинен бути обов'язково захищеним, для зменшення вірогідності витоку чи крадіжки інформації, що передається в мережі. З урахуванням досвіду проведення ООС, на сьогодні безпека інформації, яка передається мережею є однією з найважливіших складових роботи офіцера-зв'язківця у будь-якому підрозділі, що відповідає за забезпечення зв'язку пункту управління.

Виходячи з вищезазначеного, одним з найбільш використовуваних і ефективних рішень є застосування технології DMVPN (Dynamic Multipoint Virtual Private Network) розробленої компанією Cisco Systems для створення віртуальних приватних мереж та є подальшим розвитком технологій VPN (Virtual Private Network), і ґрунтується на спільній роботі протоколу NHRP (Next Hop Resolution Protocol), протоколу тунелювання mGRE (Multipoint Generic Routing Encapsulation), шифрування IPSec (Internet Protocol Security) і протоколів динамічної маршрутизації: RIP (Routing Information Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol), BGP (Border Gateway Protocol).

Дана технологія може бути розгорнута як спільно з системами безпеки Cisco IOS Firewall і Cisco IOS IPS (Image Packaging System), так і разом з такими необхідними в сучасних мережах механізмами як QoS (quality of service), IP Multicast, Split Tunneling і механізмами резервних маршрутів. Використання Cisco DMVPN дає можливість створювати великі VPN мережі з десятками і сотнями вузлів, з можливістю балансування завантаження каналів і резервування. При цьому немає необхідності вручну конфігурувати кожне з'єднання між вузлами мережі так, як з'єднання встановлюється автоматично відповідно з політиками доступу і безпеки.

Висновок

Таким чином, у ході проведення дослідження було реалізовано метод віддаленого доступу на основі технології DMVPN та проведено аналіз протоколів захисту за їх типом, призначенням та способом реалізації з метою визначення найбільш досконалого варіанту використання даної технології у Збройних Силах України. Технологія DMVPN є перспективною і актуальною для створення тунелів віддаленого доступу до мереж передачі даних в інтересах спеціальних користувачів.

к.т.н.Татарінов А.С.
к.т.н. Масесов М.О.

ПІДВИЩЕННЯ ПРОПУСКНОЇ СПРОМОЖНОСТІ ТРАНСПОРТНИХ МЕРЕЖ, ПОБУДОВАНИХ НА ОБЛАДНАННІ СТАНДАРТУ IEEE 802.11 ШЛЯХОМ ВДОСКОНАЛЕННЯ ПРОТОКОЛУ ДОСТУПУ НА MAC РІВНІ

На теперішній час для побудови транспортних мереж у системі військового зв'язку достатньо широке використання знайшли технології стандарту IEEE 802.11. Розроблені як бездротові технології доступу, за останній час отримали нові риси та можливості, у тому числі в збільшенні пропускної спроможності (табл. 1).

Таблиця 1

Показники	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6
Ширина каналу (MHz)	20, 40	20, 40, 80, 80 + 80, 160	20, 40, 80, 80 + 80, 160
Смуга частот	2.4 and 5 GHz	5 GHz	2.4 and 5 GHz
Максимальна швидкість	150 Mbps	3.5 Gbps	9.6 Gbps
Найвища схема модуляції на ортогональної частоті	64-QAM	256-QAM	1024-QAM
Кількість просторових потоків (Spatial streams)	1	4	8
Underlying technology	IEEE 802.11n	IEEE 802.11ac	IEEE 802.11ax

Застосування 802.11xx в транспортних мережах є малоефективним в термінах надійності зв'язку, пропускної спроможності, захищеності. Основними проблемами прийому/передачі в радіоканалах, у тому числі в радіоканалах технологій стандарту 802.11 в діапазоні 2 – 6 ГГц, є багатопроміневість розповсюдження радіохвиль та селективні завмирання. У каналі із завмираннями, як відомо, прямий сигнал істотно ослаблений, фаза коефіцієнта передачі рівно ймовірно розподілена, а амплітуда підпорядковується релеєвскому розподілу.

Прийняті в технології 802.11 протоколи доступу на MAC рівні дуже сильно обмежують потенційні можливості мереж, в тому числі пропускної спроможності таких мереж.

Завдання забезпечення необхідної пропускної спроможності транспортних мереж з використанням технологій 802.11 із збереженням їх стійкості фактично полягає у тому, щоб застосовувати механізми ефективного використання енергії багатопроменевого сигналу, а також використовувати такі процедури доступу, механізми обробки пакетів, кодів та видів модуляції, які найбільш „узгоджені" з параметрами багатопроменевого релеєвського каналу.

Як відомо, основною причиною значного зниження швидкості передачі даних в каналах стандартів 802.11 (throughput) на Ethernet інтерфейсі в порівнянні зі швидкістю кодування (data rate) є висока велика частка службової інформації (overhead) в пакеті Ethernet стандарту IEEE 802.11 a/g. Це призводить до того, максимальна пропускна спроможність Wi-Fi обладнання стандарту IEEE 802.11a/g на довгих пакетах порядку 1000-1500 байт становить приблизно половину від максимальної швидкості кодування символів на швидкості 54 Мбс.[1]. При зменшенні довжини пакетів даних негативний вплив службової частки збільшується так, що, наприклад, пропускна спроможність обладнання Wi-Fi 802.11a/g на дрібних пакетах довжиною 64 байт становить приблизно 16 % від пропускної спроможності на довгих 1000-1500 байт пакетах, тобто не перевищує величини 4,5 Мбс (рис.1).

Причиною такого явища є, те що та реальних каналах з завмираннями використання в EEE 802.11 a/g протоколу випадкового колізійного методу доступу (MAC рівень) до середовища, або CSMA/CA (Carrier Sense Multiple Access with Collision, Avoidance)

призводить до постійних запитань на повтор передачі (сприймає завмирання як пропуск пакету). Кількість запитань на коротких пакетах зростає дуже сильно.

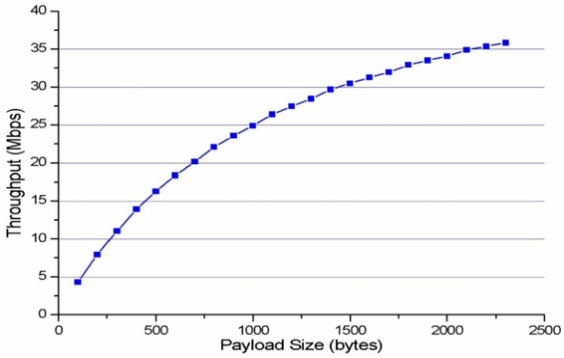


Рис. 1 Максимальна пропускна спроможність Wi-Fi обладнання стандарту IEEE 802.11a/g в залежності від довжини пакету

В пристроях стандарту IEEE 802.11n, які використовуються в транспортних мережах систем військового зв'язку, для зменшення впливу довжини пакетів на пропускну спроможність мереж, здійснена програмна агрегація пакетів даних в фрейми (Aggregated MAC Service Data Unit, A-MSDU) довжиною 4-8 Кбайт. У зв'язку з цим пристрої IEEE 802.11n мають більшу, в порівнянні з пристроями стандарту IEEE 802.11a/g, пакетну продуктивність і, як наслідок, більшу пропускну спроможність, в тому числі на дрібних пакетах. Наприклад, для обладнання 802.11n в документації вказуються параметри пропускної спроможності (швидкості кодування даних) до 85 Мбс в дуплексі на модуляції 64QAM 5/6 в каналі шириною 40 МГц MIMO 2x2, швидкість кодування даних – 270 Мбс. Але на практиці наведені цифри максимальної пропускної спроможності на Ethernet інтерфейсі пристроїв 802.11n, по-перше, значно менше швидкості кодування (data rate) на wireless інтерфейсі Wi-Fi обладнання, яка зазвичай вказується в специфікаціях на обладнання, а по-друге, пропускна спроможність в стандарті 802.11n хоча є вищою в порівнянні до показників стандарту 802.11 a/ g, але все ж таки сильно залежить від довжини пакетів даних. Таким чином, відносно високі максимальні швидкості передачі даних на обладнанні 802.11n можуть бути отримані тільки на трафіку з довгими пакетами даних, до якого можна віднести сервіс копіювання файлів за протоколом FTP. Реальна пропускна спроможність Wi-Fi пристроїв на трафіку з дрібних і середніх по довжині інформаційних пакетів в десятки разів менше, ніж максимальні швидкості передачі даних, що отримуються на тестах з копіювання файлів. Дуже важливим є той факт, перевірений на практиці (Табл 2), що використання методу просторового кодування, або MIMO 2x2, практично не приводить до підвищення пропускної спроможності.

Таблиця 2

Довжина пакету UDP, Byte	Пропускна здатність, карта RB411AH/RS2Hn Duplex Mbps		Пропускна здатність, карта Rocket M5 Duplex, Mbps			
	Ширина каналу 20MHz, SISO Tx/Rx Rate 130/130	Ширина каналу 20MHz, MIMO 2x2 Tx/Rx Rate 130/130	Ширина каналу 20 MHz, MIMO 2x2 Tx/Rx Rate 130/130		Ширина каналу 40 MHz, MIMO 2x2 Tx/Rx Rate 243/243	
			Дуплекс	Симплекс	Дуплекс	Симплекс
1470	23.9	49.1	39.1	17.3	77.1	21.9
256	17.2	17.9	20.4	4.2	21.4	4.5
160	13.2	12.6	13.3	2.6	14.2	2.8
64	7.6	6.8	5.7	1.2	6.0	1.2

З аналізу даних в (табл. 2), можна зробити висновки:

Пропускна спроможність пристроїв IEEE 802.11n на дрібних пакетах практично не залежить від ширини каналу зв'язку (20 або 40 МГц);

Пропускна спроможність пристроїв IEEE 802.11n фактично не залежить від переходу на використання замість одного каналу (SISO) на схему двох каналів (MIMO 2x2).

Проведені тестування, описані в [2] показують, що на коротких пакетах є дуже велика різниця між швидкістю передачі даних на wireless інтерфейсі та на Ethernet 10/100 BaseT інтерфейсі. Заміна на більш потужний процесор не збільшує суттєво пропускну спроможність. Результат впливу довжини пакетів на пропускну спроможність при передачі мульісервісного трафіка (4 відео потоки) по каналу обладнання стандарту 802.11 n показано на рис. 2.

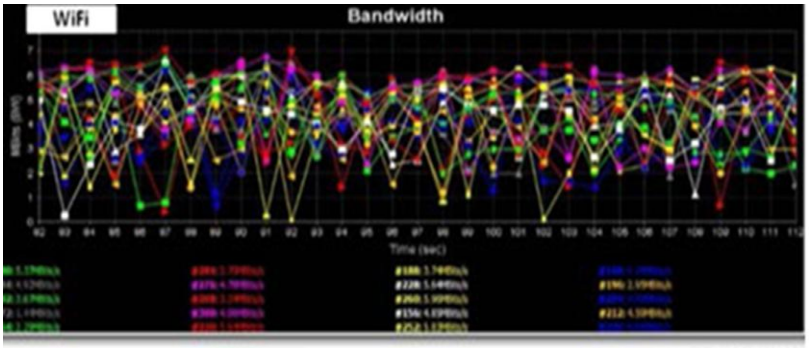


Рис. 2

Рисунок ілюструє постійне коливання швидкості передачі усіх чотирьох відео потоків протягом часту передачі.

Основна причина – пакетна продуктивність пристроїв Wi-Fi стандарту IEEE 802.11n, і як наслідок ПС, гальмується на MAC канальному рівні при перетворенні форматів пакетів даних стандарту IEEE 802.11n в формат пакетів даних MSDU IEEE 802.3 на Ethernet інтефейс і назад.

Аналіз технічних рішень, впроваджених в останніх поколіннях стандарту 802.11, а саме 802.11 ac та 802.11 ax, показують, що підвищення пропускнї спроможністі в мережі доступу може бути отримано за рахунок впровадження:

– протоколу випадкового доступу на MAC рівні но основі кадру управління (тригера) для UL OFDMA;

– технології MU-MIMO (multi-user MIMO);

– схеми модуляції QAM 1024 на відстанях до 20 метрів;

– технології beamforming – фокусування сигналу Wi-Fi в напрямку розміщення користувача;

– розширення смуг каналів (до 80 та 160 МГц).

Але ці новації суттєво не змінили базовий протокол доступу на MAC рівні. Тому вони, як й решта стандартів 802.11 мають ефект при використанні в приміщеннях на відстанях до 30 метрів. З метою пошуку шляхів боротьби з цим явищем, був проведений експеримент [2] зі встановлення на типову апаратну платформу x86 CPU Geode 500 MHz замість програмного забезпечення з драйвером протоколу IEEE 802.11 другого програмного забезпечення, яке реалізує не протокол полінгового типу, а саме **синхронний протокол TDD**. В цьому протоколі передача пакетів здійснюється за часовим графіком (протягом фіксованого кванта часу). Синхронний протокол TDD і велика частина завдань диспетчеризації обслуговування абонентів, найбільш чутливих до затримок, реалізується апаратно на канальному рівні в окремому модемі.

З'ясувалося, що на відміну від протоколу, реалізованому у чистому стандарті 802.11, пропрієртарний синхронний TDD протокол має малий обсяг службового трафіка, що забезпечує на потужній апаратній платформі високу пакетну продуктивність (близько 200 тис пакетів за секунду). При цьому пропускна спроможність практично не залежить від довжини пакета даних (табл. 3).

Таблиця 3

Тип пристрою	Ширина каналу, MHz	Пропускна спроможність,MBps UDP 64 bytes duplex	Пакетів в секунду
UBNT NS 5 IEEE 802.11a	20	0.96	4K
RB411AH/CM9 802.11a Nstreme Frame Policy 3200	20	9.7	39k
RB411AH/R52Hn 802.11n MIMO 2x2 Nstreme Frame Policy 3200	20	4.5	18 K
UBNT NS M5 802.11n MIMO 2x2	20	5.1	28K
UBNT NS M5 802.11n MIMO 2x2	40	5.6	28K
UBNT Rocket M5 802.11n MIMO 2x2	20	5.7	28K
UBNT Rocket M5 802.11n MIMO 2x2	40	6.0	28K
RB411AH/R52Hn IEEE 802.11n SISO	20	7.6	28K
RB411AH/R52Hn IEEE 802.11n MIMO 2x2	40	6.8	28K
RB800/R52Hn IEEE 802.11n, MIMO2x2, 100 BaseT	40	6.9	28K
RB800/R52Hn IEEE 802.11n, MIMO2x2, 1000 BaseT	40	14.8	60K
IEEE 802.11n, 100 BaseT TDD, MIMO 2x2	20	51.41	200K

На рис. 3 наведений практичний результат від заміни протоколу IEEE 802.11 на пропрієртарний синхронний протокол TDD. Зверху зображення з екрана комп'ютера – результат нестабільної передачі чотирьох потоків відео по каналу з протоколом IEEE 802.11 по реальному каналу зв'язку на відстані 3 км. Знизу – ілюстрація стабільного прийому усіх чотирьох відео потоків з використанням протоколу доступу TDD на MAC рівні.

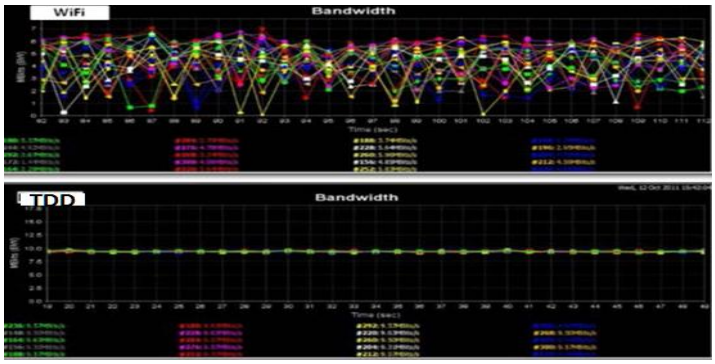


Рис. 3

Таким чином, синхронний TDD протокол доступу на MAC рівні має низький обсяг службового трафіка, що може забезпечити на потужній апаратній платформі високу пакетну продуктивність близько 200 тисяч пакетів в секунду й вище, при цьому пропускна спроможність практично не залежить від довжини пакета даних трафіка.

Застосування TDD протоколів доступу на канальному рівні на реальних каналах в діапазоні 5 ГГц не здатне усунути другу проблему – міжсимвольну інтерференцію, що має місце на фізичному рівні, хоча й підвищує стійкість роботи обладнання за рахунок використання ефективних механізмів повтору передачі при втраті або спотворенні пакетів даних від впливу інтерференції. Ефективним механізмом боротьби з міжсимвольною інтерференцією є використання метода ортогональної частотної модуляції (OFDM) з значною (більш ніж 64, що реалізовано в 802.11n) кількістю субчастот, що дозволяє зменшити швидкість передачі на кожну суб частоту, підвищити захисний міжсимвольний інтервал.

ЛІТЕРАТУРА

1. Y. Kim, S. Choi, K. Jang, H. Hwang "Throughput Enhancement of IEEE 802.11 WLAN via Frame Aggregation".:. Multimedia & Wireless Networking Laboratory School of Electrical Engineering Seoul National University 2004

2. Васильев В.Г. Анализ применения оборудования Wi-Fi стандарта IEEE 802.11a/b/g/n (чистого Wi-Fi) в сетях фиксированного безпроводного широкополосного доступа.:. Юнітата, 2010.

Троценко О.Я. (НАСВ)
Середенко М.М. (НАСВ)

ПІДГОТОВКА КУРСАНТІВ ВИЩИХ ВІЙСЬКОВИХ НАВЧАЛЬНИХ ЗАКЛАДІВ ДО ВИКОНАННЯ БОЙОВИХ ЗАВДАНЬ В ЕКСТРЕМАЛЬНИХ УМОВАХ

Практика ведення сучасних збройних конфліктів, в тому числі і досвід ведення бойових дій на Сході України показує, що у більшості молодих офіцерів психологічна підготовленість до дій в екстремальних умовах бойової діяльності значною мірою не відповідає необхідним вимогам. Виконуючи військово-професійні завдання під впливом негативних факторів, які супроводжують навчально-бойову і бойову діяльність, багато хто з них часто ніяковіє, погано орієнтується в обстановці, що склалася, проявляє невпевненість в управлінні підлеглим особовим складом, недостатньо ефективно використовує свою штатну зброю та бойову техніку. Причиною цього, в більшості випадків, є недостатня психологічна підготовка до виконання професійних обов'язків в екстремальних умовах.

Актуальність питання про удосконалення процесу підготовки курсантів вищого військового навчального закладу (ВВНЗ) – майбутніх офіцерів, до виконання професійних обов'язків, зумовлена ускладненням нинішніх умов проходження військової служби. При виконанні завдань за призначенням, коли військовослужбовці знаходяться під впливом вельми значних за силою і потужністю психологічних подразників, дуже важливо з самого початку служби (навчання) підготувати їх фізично і психологічно, сформувати здатність управляти своїми відчуттями і поведінкою, з високою точністю і надійністю виконувати складні професійні (бойові) дії.

З метою формування особистості майбутнього офіцера, як командира військового підрозділу, фахівця з конкретної військової спеціальності з високим рівнем, психологічної підготовленості та емоційної стійкості доцільно впроваджувати у навчальний процес курсантів ВВНЗ новітні форми і спеціальні методи навчання, в тому числі – активне та інтерактивне навчання із застосуванням комп'ютерних технологій з елементами імітаційного моделювання. Процес навчання майбутніх офіцерів з використанням сучасних технологій для моделювання бойових дій повинен сприяти формуванню в індивідуальній свідомості кожного курсанта алгоритмів успішно діяти в екстремальних умовах та мати практичну спрямованість.

Сутність спеціальних методів підготовки курсантів полягає в організації пошукової, творчої діяльності тих, хто навчаються щодо вирішення нових для них проблем. Для досягнення цієї мети керівником заняття відпрацьовується спеціальний комплекс завдань, направлених на формування готовності до дій в екстремальних ситуаціях, на групових вправах, тактичних заняттях створюється складна, нестандартна обстановка, місцевість незнайома, противник застосовує несподівані (нові) способи бойових дій або застосовує нову зброю. Слухачі, при цьому, ставляться в умови, коли від них потрібно швидко прийняти нешаблонне, оригінальне рішення на бій, на застосування нового способу використання зброї і бойової техніки, нового способу бою для протидії противнику. Слухачі самостійно, без підтримки викладача, повинні вирішувати проблемні завдання, що виникли.

Для розробки моделей спеціальної підготовки курсантів до дій в екстремальних умовах бойової обстановки необхідно застосовувати наступні рекомендації.

При проведенні занять (групових вправ і польових занять):

– формування структури (методики) проведення занять, що включає теоретичні і практичні заняття з загальновійськових дисциплін;

– використання спеціальних інтелектуальних завдань, що вирізняються складністю та глибиною, з врахуванням етапності їх засвоєння згідно принципу «від простого до складного»;

– введення комплексу контрольно-тренувальних вправ системи БАрС під час проведення практичних занять з вогневої, тактичної, фізичної підготовки та занять з тактичної медицини протягом всього періоду навчання.

При розробленні (моделюванні) інтелектуальних завдань доцільно дотримуватися алгоритму, який забезпечує високий рівень ефективності підготовки, з врахуванням основних дидактичних правил організації процесу навчання:

1. Відповідність змісту екстремальних ситуацій навчальним завданням, які моделюються доцільно забезпечувати за рахунок використання наступних критеріїв:

– умови виконання завдань мають бути максимально наближені до бойових;
– відображати конкретні екстремальні ситуації;
– врахувати особливості основної професійної діяльності (обраної спеціалізації);
– викликати інтерес у тих, хто навчається;
– відповідати кваліфікації військовослужбовців;
– мати доступні та перевірені механізми вирішення.

2. Умови реалізації інтелектуальних завдань і моделей практичної діяльності в навчально-бойовій обстановці складати на основі визначених компонентів:

– конкретні показники зовнішньої обстановки, труднощі, які необхідно подолати, час, протягом якого слід вирішувати завдання;
– проведення теоретичних занять з використанням інтелектуальних завдань, які характеризуються специфічними умовами професійної діяльності (спеціалізації);
– подолання екстремальних ситуацій способами з мінімальними втратами для життя і здоров'я та з врахуванням часу;
– теоретичні моделі екстремальних ситуацій доцільно надавати, як в усній, так і в письмовій або електронній (ігровий) формі;
– додаткові відомості, що роз'яснюють умови виконання завдань, положень, що пропонуються, повинні міститися в спеціальних інформаційних виданнях, доступних для тих, хто навчається;
– процес вирішення завдань повинен виключати групові обговорення – кожен курсант зобов'язаний знаходити відповідь самотужки.

3. Під час проведення практичних занять, важливо пам'ятати наступне:

– метою проведення практичних занять є закріплення отриманих під час теоретичних занять знань, формування і вдосконалення практичних умінь і навиків діяти в екстремальних умовах бойової діяльності;
– навчальний матеріал повинен складати практичні моделі екстремальних умов, які відповідають змісту інтелектуальних завдань, що використовувалися на теоретичних заняттях;
– практичні уміння і навики краще формуються і удосконалюються в умовах, максимально наближених до навчально-бойової обстановки, з врахуванням особливостей військово-професійної спеціалізації;
– наприкінці практичних занять слід проводити спеціальні заходи, які направлені на відновлення психічних, інтелектуальних і рухових можливостей тих, хто навчається;
– при проведенні практичних занять з моделюванням екстремальних умов необхідно дотримуватися вимог техніки безпеки та забезпечити обов'язковий медичний контроль для надання допомоги (за необхідністю).

Отже, запропонована модель підготовки курсантів, застосування нових активних форм та методів навчання, проведення занять з навчальних дисциплін та предметів бойової підготовки в умовах психологічного навантаження шляхом моделювання негативних чинників бою сприяє формуванню у курсантів знань і навичок необхідних для професійної роботи, дозволить підвищити якість підготовки фахівців, успішно формувати у військового професіонала важливих якостей „офіцера – командира", „офіцера – лідера".

Турпітько Б.М. (ВІТІ)
Тетерятник І.В. (ВІТІ)

АВТОМАТИЗОВАНЕ РОБОЧЕ МІСЦЕ ПОСАДОВОЇ ОСОБИ СЛУЖБИ РАКЕТНО-АРТИЛЕРІЙСЬКОГО ОЗБРОЄННЯ

Дослідивши керівні документи посадової особи служби ракетно-артилерійського озброєння (РАО), а також ознайомившись з подібними документами сфери ракетно-артилерійського озброєння, стало відомо, що робоче місце посадової особи служби РАО потребує вдосконалення. Було прийнято рішення, що до створення програмного додатку для автоматизації робочого місця. Зважаючи на те, що посадова особа працює з великою кількістю подібної інформації, ефективно було б створити програмне забезпечення для прискорення, управління та контролю інвентаризації майна служби ракетно-артилерійського озброєння.

Створений додаток буде взаємодіяти з користувачем та виконувати функції зберігання, редагування, пошуку занесеної інформації. Використання додатку дозволить автоматизувати роботу посадової особи служби ракетно-артилерійського озброєння, забезпечить високу швидкість додавання та видалення оскільки інформаційне забезпечення є одним із ресурсів Збройних сил України і належить до основних складових системи управління. прийняття виважених управлінських рішень можливе лише на основі інформації.

Вихідними даними програмного модуля є: готовий програмний додаток, орієнтований на місце посадової особи служби ракетно-артилерійського озброєння. Даний web-додаток включає всю зазначену інформація військового майна ракетно-артилерійського озброєння згідно документів та форм що заповнюються підрозділом ракетно-артилерійського озброєння.

Перевагами використання програмного модулю є:

1. Швидке редагування відсортованої інформації згідно документообігу.
2. Прискорення проведення інвентаризації майна.
3. Зручна авторизація користувача, та надання йому повноважень.
4. Простота розгортання.
5. Високий рівень розвитку і надійності мережевих з'єднань і web-технологій.

Додаток буде створено з сервісів які будуть взаємодіяти з користувачем та виконувати певні функції такі як зв’язок між посадовою особою та підлеглими, доступ до бібліотеки матеріалів, проведення тестувань тощо. Планується реалізувати моніторинг змін останніх даних. Вносити дані про оцінки зможе лише користувач що має додаток з відповідним акаунтом.

Висновок в цілому процес розгортання системи управління ЗС України відбувається поетапно з поступовим запровадженням стандартів НАТО. Саме тому вживаються заходів для пришвидшення вирішення завдань зі створення та запровадження ЄАСУ (єдиної автоматизованої системи управління, програмної платформи, сумісної з НАТО).

В роботі було проведено аналіз/дослідження посадової особи служби ракетно-артилерійського озброєння та автоматизація його роботи. Розроблено ефективний спосіб організації обліку озброєння, що передбачає створення гнучкої, багатофункціональної системи, орієнтованої на забезпечення вихідною інформацією користувачів з метою прийняття виважених управлінських рішень та прискорення інвентаризації майна, проаналізовано основні документи, якими регламентується робота командирів підрозділів ракетно-артилерійського озброєння для збирання інформації з подальшим використанням в необхідному напрямку; розроблено програмний модуль системи обліку військового майна для посадової особи служби ракетно-артилерійського озброєння; проаналізовано методику використання створеного web-додатку. Проведено тестування та аналіз ефективності згідно керівних документів.

Фесьоха Н.О. (ВІТІ)
Гелета Д.Р. (ВІТІ)

ПРОГРАМНИЙ МОДУЛЬ ОБЛІКУ ОСОБОВОГО СКЛАДУ ВВНЗ НА ОСНОВІ ЧАТ-БОТУ

Облік особового складу є невід'ємною і обов'язковою складовою служби у ЗСУ. Одним з основних завдань обліку – є постійне знання начальниками наявності підлеглого особового складу [1, 2]. Для організації даного виду обліку курсантів у ВВНЗ використовується застарілі способи, з використанням паперових носіїв інформації, що затратно як матеріально, так і по часу. Таким чином, постає питання на знаходження альтернативних методів і способів для автоматизації оновлення інформації про наявність і місцезнаходження курсантів і оперативне отримання цієї інформації командирами, використовуючи сучасні інформаційні технології.

Пропонується здійснити розробку модулю обліку особового складу ВВНЗ на основі чат-боту. Використання чат-боту месенджера вирішує питання розробки кросплатформного додатку із зручним інтерфейсом та роботою в мережі.

Модуль представляє собою систему збору і обробку даних. Найбільш поширеною реалізацією розподіленої системи збору та обробки даних є багаторівнева система безпеки, архітектура якої базується на використанні датчиків (сенсорів) на рівні даних, сервісів управління на рівні управління даними, серверів (сервісів) збору і обробки даних на системному рівні, АРМ і контролера безпеки на рівні користувачів.

Засновуючись на архітектурі системи безпеки, пропонується використовувати трирівневу архітектуру (рис. 1). На першому рівні знаходится месенджер, який виконує функції джерела даних і їх графічне відображення. На другому рівні знаходиться сервер чат-боту, яких перенаправляє дані між месенджером і сервером збору і обробки даних в обох напрямках. На третьому рівні знаходиться сервер збору і обробки даних, яких взаємодіє з системою керування базою даних та повертає користувачам результати їх запитів.

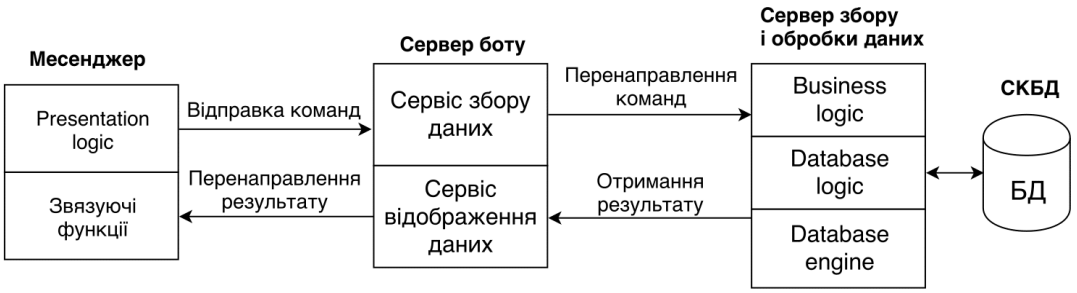


Рис. 1

Реалізований, на основі чат-боту, модуль можна використовувати в інституті, як самостійну систему, для збору інформації про наявність і місцезнаходження особового складу командною і черговою ланками. Крім того, на основі статистики наявності військовослужбовців, командири мають змогу приймати рішення для розподілу службових обов'язків, складати графік чергувань і т. д.

Використання такого способу обліку наявності та місцезнаходження особового складу значно пришвидшує процес збору і відображення даних і автоматизує ведення статистики.

ЛІТЕРАТУРА

1. Інструкція з організації обліку особового складу Збройних Сил України [Електронний ресурс].– Режим доступу URL: https://zakon.rada.gov.ua/laws/show/z0611-14

2. Статут внутрішньої служби Збройних сил України [Електронний ресурс].– Режим доступу URL: https://zakon.rada.gov.ua/laws/show/548-14.

Філіпов В.В. (ВІТІ)
Денгін О.Г. (ВІТІ)
Мотрич А.В. (А0565)

ПЕРСПЕКТИВИ УДОСКОНАЛЕННЯ ЗАСОБІВ ПРОВОДОВОГО ТА ВОЛОКОННО - ОПТИЧНОГО ЗВ'ЯЗКУ В МЕХАНІЗОВАНОМУ БАТАЛЬЙОНІ.

Проводовий зв'язок у механізованому батальйоні організовується в оборонному бою, у вичікувальному районі при прориві оборони противника з ходу, у вихідному положенні для наступу, коли батальйон прориває оборону з рубежу безпосереднього зіткнення із противником, а також для забезпечення внутрішнього зв'язку на командно-спостережному пункті батальйону.

Основним способом організації проводового зв'язку в мб є напрямок до командирів підлеглих підрозділів (механізованих рот, мінометної батареї і ін.).

Проводовий зв'язок між підрозділами батальйону здійснюється через ВЗ КСП батальйону.

У ході наступу проводовий зв'язок у батальйоні, як правило, не організовується, але всі проводові засоби зв'язку повинні перебувати в постійній готовності до розгортання у випадку різкої зміни обстановки, коли темп наступу підрозділів сповільнюється (наприклад, на рубежах тривалого зіткнення із противником, при форсуванні водних перешкод і при переході від наступу до оборони).

При наступі з висуванням із глибини) проводовий зв'язок у мб організовується у вичікувальному районі кабелем П-274М. Через нетривале перебування підрозділів у вичікувальному районі проводовий зв'язок від КСП мб організовується за скороченою схемою, тобто по одній проводовій лінії зв'язку із двома або трьома ротами. Як правило, у вичікувальному районі від КСП батальйону розгортається 2 – 3 напрямки проводового зв'язку, по яких забезпечується зв'язок з усіма підрозділами.

Проводовий зв'язок з командним пунктом бригади забезпечується по напрямку, що розгортається силами і засобами польового вузла зв'язку бригади (відповідно до розпорядження по зв'язку штабу бригади). Як правило, цей напрямок зв'язку (кабелем П-274М) розгортається від ВЗ КП бригади через КСП батальйону до вихідного пункту на маршруті висування батальйону.

Основним способом організації проводового зв'язку в батальйоні є напрямок.

Проводовий зв'язок командира і штабу мб із командиром і штабом бригади розгортається за напрямком розпорядженням із зв'язку штабу бригади силами та засобами польового вузла зв'язку бригади (кабелем П-274М). А з командирами механізованих рот та інших підрозділів батальйону від КСП мб силами і засобами взводу зв'язку батальйону (кабелем П-274М).

Для організації проводового зв'язку у взводі зв'язку мб є: легкий польовий кабель П-274М – 25 км; польовий телефонний комутатор П-193М (ТК-1) – 2 комплекти; польовий телефонні апарати ТА-57=20 комплектів.

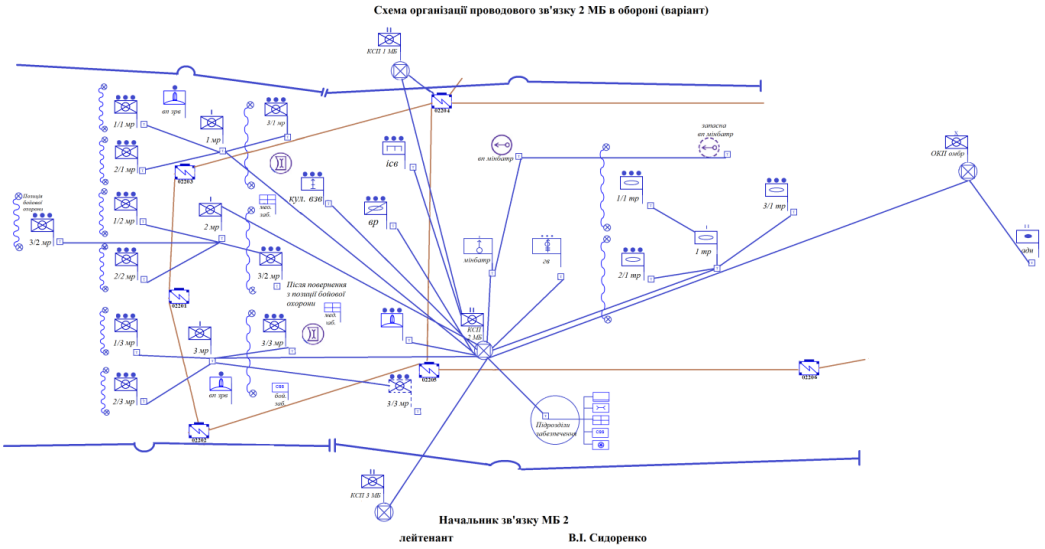
З метою забезпечення більшої живучості проводових ліній зв'язку вони розгортаються з урахуванням захисних властивостей місцевості по траншеях, ходах сполучень в стороні від маршрутів руху гусеничної техніки або заглиблюються в землю.

На пунктах управління та на підходах до них всі проводі лінії зв'язку, як правило, заглиблюються в землю, або прокладаються в рівчаках і маскуються. Проводовий зв'язок з командиром і штабом мбр забезпечується силами і засобами польового вузла зв'язку мбр за напрямком у відповідності з розпорядженням із зв'язку штабу мбр через запасні місця розгортання ПУ мбр і мб.

В батальйоні проводовий зв'язок організовується від КСП мб з командирами механізованих рот, мінометною батареєю (ПТВ для мб на БТР) зенітно-ракетного взводу, гранатометного і розвідувального взводів, ротою матеріального забезпечення, інженерно-

саперним взводом, медичним пунктом,постом позначення батальйону, пунктом технічного спостереження за напрямком силами і засобами вузла взводу зв'язку мб. Також передбачається організація проводового зв'язку з бойовою охороною, бронегрупою, вогневими засідками і командирами приданих підрозділів, які перебувають в безпосередньому підпорядкуванні командира мб.

Проводовий зв'язок взаємодії з іншими батальйонами бригади, елементами його бойового порядку встановлюється через ВЗ КП бригади і БРАГ. В деяких випадках, при наявності достатнього часу і засобів зв'язку, може встановлюватися проводовий зв'язок за напрямками із КСП сусідніх батальйонів (засобами правого сусіда).



Перспективи розвитку та шляхи удосконалення розвитку засобів проводового та волоконно-оптичного зв'язку

В провідних країнах світу в інтересах вдосконалення системи зв'язку з'єднання розробляється та впроваджується комплекс технічних засобів, призначений для оперативної побудови цифрової мережі проводового зв'язку в польових умовах.

Розробка та використання переносних волоконно-оптична система зв'язку з розподіленою комутацією для тактичної ланки управління дозволить оперативно розгортати цифрові мережі і напрямків провідний, волоконно-оптичної та оптичного зв'язку з організацією ліній прямого телефонного зв'язку, автоматичної комутацією абонентів, виходом в телефонну мережу загального користування, дистанційним керуванням радіо засобами підрозділів і роботою по радіо в мережах рухомого зв'язку. При цьому необхідно відзначити, що підвищення надійності ліній проводового зв'язку досягається за рахунок застосування оптичного зв'язку і радіозв'язку.

В даний час розгорнуті роботи по оснащенню сучасними комплексами засобів автоматизації управління командних пунктів, в тому числі і тактичної ланки управління.

В ЗСУ на даному етапі відбувається широке використання кабельних цифрових модемів на мідних та волоконно-оптичних кабельних мережах; поступовий перехід на волоконно-оптичні лінії зв'язку, що значно збільшує пропускну спроможність передачі інформації; проведення переобладнання, власними силами, апаратних старого парку типу П-258, П-256, П-240, П-241, П-238 та П-178, що дозволить забезпечити керівний склад на відповідних пунктах управління сучасними телекомунікаційними послугами; використання прийнятих на озброєння ЗС України комплексних апаратних зв'язку К-1501 з подальшим їх удосконаленням. Пропонується підвищення пропускної спроможності і збільшення протяжності регенераційних ділянок магістральних ліній зв'язку та ліній прив'язки, підвищення їх стійкості до впливу деструктивних чинників електромагнітної природи, використання спектрального ущільнення оптичних сигналів, зниження втрат в лінійному оптичному тракті, підвищення енергетичного потенціалу волоконно-оптичних ліній зв'язку.

д.т.н. С.П. Фриз (ЖВІ)
к.т.н. О.В. Кальватинський (ЦПОСІ та КНП)
Р.О. Авсієвич (ЖВІ)

ВИКОРИСТАННЯ КОСМІЧНИХ АПАРАТІВ ТИПУ «CUBESAT» У СКЛАДІ КОСМІЧНИХ СИСТЕМ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

Досвід проведення Операції об'єднаних сил вказує на те, що ефективне застосування наземних сил неможливе без використання космічних засобів для підтримки військових операцій. Однак, на даному етапі, Україна не має у своєму розпорядженні власних космічних апаратів (КА) та вимушена використовувати орендований бортовий ресурс у країн партнерів, міжнародних операторів та приватних компаній. Вирішення даної проблеми можливе через використання „наносупутників" типу „CubeSat". Так, розробкою та дослідженнями КА типу „CubeSat" займаються більше 100 наукових установ, державних та приватних компаній у 77 країнах світу. Зокрема, значні напрацювання мають США, Канада, Австралія, Великобританія, Китай, Російська Федерація, Данія, Франція, Німеччина, Індія, Ізраїль, Італія, Японія, Литва, Нідерланди, Південна Корея, Іспанія та Швейцарія. Основною перевагою КА типу „CubeSat" є низька вартість запуску, яка залежно від розмірів та ваги, лежить в ціновому діапазоні від 3000 до 80 000 доларів США. Аналіз доступних зарубіжних джерел інформації дозволив встановити, що КА типу „CubeSat" активно використовуються для забезпечення телекомунікаційних послуг. Так, 24.05.2019 компанією „SpaceX" на низьку навколоземну орбіту виведено 60 КА типу „CubeSat" в рамках проєкту „StarLink". Відповідно до планів компанії більше 50 % трафіку, що передається в рамках функціонування мережі „Інтернет", буде проходити через мережу „StarLink". КА типу „CubeSat" використовуються і в оборонній сфері. Зокрема, доступні джерела інформації містять дані, що подібні КА експлуатуються оборонними відомствами США, Австралії, Колумбії, Нідерландів і Таїланду. Основним призначенням вказаних КА є забезпечення телекомунікаційних послуг, дистанційне зондування Землі, збір даних з наземних сенсорів, протиракетна оборона та контроль космічного угруповання. В майбутньому, оператори КА типу „CubeSat" планують зменшити вартість їх виведення на орбіту, збільшити термін експлуатації та швидкість обміну даними, покращити роздільну здатність космічної зйомки тощо. Відповідно до бази даних „Nanosats.eu" з 2019 року на низьку навколоземну орбіту планується виводити близько 500 нових „наносупутників» щороку, в тому числі „CubeSat". Україна також здійснює розробки КА типу „CubeSat". Так, Національний технічний університет України „Київський політехнічний інститут ім. Ігоря Сікорського» розробив два подібні апарати, що були виведені на орбіту 19.06.2014 та 18.04.2017. Третій український супутник „DneprCubeSat" наразі перебуває на етапі розробки. Створювані КА типу „CubeSat" в Україні використовуються для наукових досліджень, але на відміну від інших країн, в Україні відсутня концепція застосування таких КА в інтересах безпеки та оборони. Аналіз наявних даних про КА дозволив встановити, що в умовах обмеженості часових та фінансових ресурсів, розгортання таких орбітальних угрупувань можливе в короткі терміни з використанням пускових послуг, які надаються країнами партнерами. Враховуючи те, що вже на даний час КА типу „CubeSat" дозволяють виконувати задачі із характеристиками, які задовольняють замовників, в найближчі п'ять років слід очікувати на значні зміни у космічному угрупованні. У зв'язку з цим, використання наносупутників, в тому числі „CubeSat", в оборонній сфері набуває більшої актуальності і потребує подальших наукових досліджень. В доповіді пропонуються способи застосування КА типу „CubeSat" для телекомунікаційного забезпечення сектору безпеки та оборони України. Крім того, подібні КА можуть оснащуватися цільовим обладнанням для здійснення моніторингу радіоелектронної обстановки, дистанційного зондування Землі, метрологічного забезпечення тощо. Поряд з цим, розглянуто шляхи створення наземної інфраструктури для управління такими КА із залученням існуючих технічних засобів, які знаходяться на території України.

д.т.н. Хлапонін Ю.І. (КНУБА)
к.т.н. Мазулевский О. Є. (ВІТІ)
к.н.д.у. Хлапонін Д.Ю. (ДУТ)

ФУНКЦІОНАЛЬНА ТА КІБЕРБЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНИХ СИСТЕМ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Кіберпростір використовується в усіх сферах життя людини, від особистого простору до державного управління, військової сфери та управління важливими елементами життєзабезпечення. Тому питання забезпечення захисту кіберпростору є актуальними.

Метою роботи є визначення та розмежування понять забезпечення функціональної безпеки та кібербезпеки інформаційно-керуючих (кіберфізичних) систем у критичних галузях, де відмови, обумовлені атаками на вразливості, фізичними і проектними дефектами, можуть призвести до значних матеріальних втрат, аварій, загрози життю та здоров'ю людей. У військовій сфері до таких систем можна віднести підсистеми зв'язку в системах автоматизації управління зброєю (ракетною, артилерійською, авіаційною і т.д.) так і саму систему зв'язку, як підсистему системи управління ЗС України.

Функціональна безпека кіберфізичних систем – властивість пов'язана зі здатністю кіберфізичних систем (КФС) забезпечити відсутність катастрофічних наслідків для життя, здоров'я, власності чи даних персоналу та зацікавлених осіб КФС та фізичного середовища.

Оскільки на сьогоднішній день в світі всі процеси в обороні, економіці, промисловості, інфраструктурі стають все більше зв'язаними, то все більш широкого застосування набувають кіберфізичні системи як інтелектуальні мережні інженерно-взаємодіючі системи, які поєднують в собі фізичні, телекомунікаційні та обчислювальні компоненти. Невід'ємною необхідною складовою функціонування кіберфізичних систем є кібербезпека, яка забезпечує надійні, безпечні, стійкі умови функціонування КФС.

Відомі визначення в Законі України „Про основні засади забезпечення кібербезпеки України" використовує термін „критично важливі об'єкти інфраструктури" та „об'єкти критичної інформаційної інфраструктури". А Європейський Союз визначає „критичну інфраструктуру" як системи, які мають важливе значення для підтримки життєво-важливих соціальних функцій. Пошкодження критичної інфраструктури, її руйнування або порушення в результаті стихійних лих, тероризму, злочинної діяльності або зловмисної поведінки, може істотно негативно вплинути на безпеку ЄС і добробут громадян.

Таким чином, для гарантування безпечного, стійкого, конфіденційного функціонування мереж об'єктів критичної інфраструктури (як КФС) в режимі реального часу першочергового значення набувають не заходи попередження і боротьби з кібератаками, несанкціонованим вторгненням до мереж хакерів. Першочергового значення набувають необхідність детального проектування об'єктів критичної інфраструктури (як КФС), введення до складу системи базових пристроїв оповіщення про порушення працездатності елементів системи, встановлення в необхідній кількості та у ключових точках системи датчиків з функціями сприйняття та повідомлення до центру управління системи про порушення номінальних показників, забезпечення фіксування при проектуванні датчиків правильного часу для своєчасного їх реагування на надзвичайні події в системі, забезпечення електромагнітної та функціональної сумісності складових мережі. Досягнення цих вимог потребує таких заходів і механізмів державного управління як сертифікація засобів зв'язку, засобів автоматизації управління в складі мереж (як КФС) із застосуванням надійних протоколів зв'язку, сертифікація функціональної сумісності мереж об'єктів критичної інфраструктури (із дотриманням вимог функціональної безпеки, безпеки доступу до КФС, стійкості, адаптивності, конфіденційності та інш.); прийняття міжнародних стандартів як національних для стандартизації часу реагування датчиків, сенсорів, виконавчих пристроїв, стандартів безпеки електропостачання, а в галузі оборони – визначених стандартів КФС для забезпечення оборони держави, захисту суверенітету та охорони державної таємниці з урахуванням напрямку євроінтеграції та вступу в НАТО закріплених в Конституції України.

д.т.н. Хорошко В.О. (ВІТІ)
Калантаєвська С.В. (ВІТІ)
Макарчук О.М. (ВІТІ)

МЕТОД КОРЕКЦІЇ ЗОБРАЖЕННЯ З БпЛА ПРИ НАЯВНОСТІ ШУМІВ ТА ЗАВАД

У теперішній час безпілотні літальні апарати (БпЛА) є основними елементами інформаційно-розвідувальними засобами забезпечення та дістанційного впливу на противника під час бойових дій, а також для забезпечення внутрішній безпеці держави. БпЛА стали обов'язковою та невід'ємною частиною Збройних сил і широко використовуються невійськовими формуваннями, у тому числі і поліцейськими підрозділами як за кордоном, так і у нас. Зараз БпЛА використовуються для вирішення оперативних завдань, та їх роль суттєво зросла під час бойових дій, правоохоронних і екологічних дій в тактичному звіні.

Процес розробки методів поновлення зображення на дисплеї оператора наземної частини комплекса, на наш погляд, стає найбільш важливим. Це пов'язано з тим, що необхідно обробляти швидко поступаючу інформацію у реальному часі та видавати на дисплей чітке та яскраве зображення, яке дозволить точно визначати місцезнаходження об'єкта та то що він собою являє.

Слід теж врахувати, що поступаюча інформація має також накладені на неї шуми та завади, що дають розмите та нечітке зображення. Тому методи локалізації контурів об'єктів становляться все більш необхідними при застосуванні БпЛА. Ефективність методів, що досягають необхідної точності, може розглядатися в двох аспектах: як засіб одержання вищої точності, або як засіб, що отримує таку ж точність за менше кроків обчислення

На сьогодні відомо ряд методів локалізації контуру об'єкта, серед яких чітке місце займає градієнтний метод і його модифікації. Подальший розвиток методів локалізації краю об'єкта привів до використання інтерполяції в межах підйому-спаду градієнта. Цей метод менш чутливий до шуму в порівнянні з іншими операторами градієнта, проте точність обмежана. Більш складна поліномінальна чи b-сплайн інтерполяція дає змогу отримати вищу точність.

На жаль всі ці методи використовують багато часу обчислення процесів та не завжди є ефективними, оскільки працють тільки в малому околі, де відбувається перетин яскравості нульового рівня, а також досить чутливі до адаптивного шуму.

Метою дослідження є розробка методу локалізації краю об'єкта спостереження на основі гауссової низькочастотної фільтрації, на основі методу корекції зображення, отримуємого з БпЛА, при наявності шумів і завад.

Проведені попередні дослідження підтверджують можливість використання для локалізації перепаду яскравості, тобто краю об'єкта на зображенні, спільних точок примежових кривих отриманих в результаті повторного згладжування зображення з одним і тим же низькочастотним гауссовим ядром.

На підставі проведених теоретичних викладок можна зробити висновок про можливість знаходження краю об'єкта на зображенні, отриманого за допомогою матричного фотоприймального пристрою та запропонувати алгоритм локалізації краю зображення, який включає такі кроки.

Крок 1. Визначення точек максимального градієнта, що відповідають перепадам якравості, а отже краю зображення.

Крок 2. Визначення орієнтації градієнта.

Крок 3. Знаходження параметрів гауссоїди за розподіленням сигналу примежової кривої на зображенні в точках максимального градієнту.

Крок 4. Формування однонаправленого гауссового фільтра з певними параметрами відповідної орієнтації в залежності від напрямку вектора градієнта.

Крок 5. Знаходження спільних точок на примежовій кривій вхідного зображення та розмитого.

Знаходження параметрів гауссоїди за розподіленням сигналу в області різкого краю у випадку наявності шумів пов'язано зі значною неоднорідністю, оскільки значення максимуму та мінімуму перепаду яскравості, а також величину градієнта визначити точно, в багатьох випадках, практично неможливо. Для усунення цієї неоднорідності необхідно виконати фільтрацію зображення тим же гауссовим фільтром, але з параметрами, що дозволять приглушити шум на зображенні.

Дисперсія сигналу в знайденому вікні приблизно приймається за дисперсію шуму на зображенні.

У реальних зображеннях виникають ситуації, коли ділянка зображення має максимальні або мінімальні значення яскравості. Тоді дисперсія сигналу дорівнює нулю при обробці зображення необхідно уникнути оцінки шуму на таких ділянках.

При визначенні дисперсії шуму необхідно враховувати й те, що реальне значення дисперсії можна знайти, тільки якщо розмір вікна збігається з розміром зображення, а зображення майже однорідне. При малому ж розмірі вікна, знайдена величина дисперсії може виявитися дуже заниженою. Тому розмір вікна повинен вибиратися виходячи з вигляду оброблюванних зображень, а сам алгоритм стає двопрохідним.

Таким чином, метод визначення краю зображення при наявності шумів включає такі кроки:

Крок 1. Визначення параметрів шуму на зображенні.

Крок 2.Виконання низькочастотної фільтрації за допомогою гауссового фільтра з певними параметрами.

Крок 3. Визначення точок максимальних значень градієнта, що відповідають перепадам яскравості краю зображення.

Крок 4. Визначення орієнтації градієнта.

Крок 5. Знаходження параметрів гауссоїди за розподіленням сигналу примежової кривої на зображенні в точках максимального градієнта.

Крок 6. Формуваня однонаправленного гауссового фільтра з певними параметрами відповідної орієнтації в залежності від напрямку вектора градієнта.

Крок 7. Знаходження спільних точок на примежовій кривій вхідного зображення та розмитого.

Координати краю синтезованого незашумленого зображення були відомими, а координати краю зашумленого зображення визначалися запропонованим методом для кожного рядка матриці. При цьому після приглушення шуму в результаті фільтрації всього зображення для кожного рядка та стовпця матриці, де знаходилась примежова крива визначилися параметри гауссоїди, тобто ступень розмиття, розмірність фільтра та його вагові коефіцієнти, за якими синтезувалися однонаправлені фільтри горізонтальні та вертикальні в залежності від орієнтації краю.

В запропонованому методі локалізації краю об'єкта на основі гауссової низькочастотної фільтрації доведено, що спільна точка примежових кривих зображень отриманих за допомогою гауссового фільтра знаходиться на рівні 0,5 максимальної яскравості перепаду. Розроблена та досліджена математична модель локалізації краю зображення з використанням синтезованого зображення з накладеним шумом.

Запропонований метод дозволяє підвищити чіткість та яскравість зображення на дисплеї оператора, яке надходить з БпЛА.

Причому, метод дозволяє знизити до внутрішніх шумів комплексу вплив шумів і завад, які накладаються на передану інформацію.

Цей метод корекції зображення, на наш погляд, може знайти широке застосування при використанні комплексів БпЛА в умовах активної радіоелектронної протидії та радіоелектронному маскуванні об'єктів.

к.т.н. Хусаінов П.В. (ВІТІ)

ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНОЇ МОДИФІКАЦІЇ ПАРАМЕТРІВ ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ ОБЧИСЛЮВАЛЬНОЇ СИСТЕМИ НА ОСНОВІ ІДЕНТИФІКАЦІЇ ЕЛЕМЕНТІВ МІКРОПРОГРАМНОГО УПРАВЛІННЯ

Успішна реалізація того чи іншого варіанту комп'ютерної атаки класу *Man in The Middle (MITM)* надає її організатору (ініціатор деструктивного кібернетичного впливу, зловмисник) широкий спектр сценаріїв (способів) для подальшої несанкціонованої зловмисної діяльності на основі можливості прихованого аналізу інформаційних потоків взаємодії між процесами оброблення даних обчислювальної системи. Здійснення *MITM* передбачає нав'язування зловмисником (на підготовчому етапі комп'ютерної атаки) такої зміни маршрутів інформаційних потоків, при якій вони будуть проходити через контрольований (несанкціоновано-впроваджений, підмінений) активний елемент (програмно-апаратний засіб) фізичної структури обчислювальної системи. Найбільш дієвим способом захисту від комп'ютерних атак класу *MITM* (зменшення ймовірності і часу використання наслідків в разі успішної реалізації підготовчого етапу) є періодичне здійснення автоматичного контролю ідентичності (близькості) поточного та еталонного вектору значень параметрів програмно-апаратних засобів (для всієї множини відомих маршрутів інформаційних потоків) обчислювальної системи.

Виходячи з викладеного, була сформульована постановка та розроблена структурно-логічна схема дослідження щодо вирішення практичної задачі виявлення несанкціонованої модифікації параметрів програмно-апаратних засобів обчислювальної системи (як функція системи кібернетичного захисту) в основу якої, покладена ідея ідентифікації (встановлення властивостей досліджуваного явища або об'єкта) моделі тракту того чи іншого маршруту при проходженні тестового інформаційного потоку. Модель тракту інформаційного потоку – послідовність агрегатів (агрегатна система) перетворення вхідних кодових комбінацій даних інформаційного потоку у вихідні, кожний з яких, забезпечуються функціонуванням елементу (сукупність програмних засобів) мікропрограмного управління операційної системи. Достатня за тривалістю послідовність вимірюваних миттєвих значень процесу електроживлення програмно-апаратного засобу є вичерпною характеристикою властивостей та параметрів відповідного агрегату елементу мікропрограмного управління.

Доповідь присвячена стислому викладенню наукових результатів дисертаційного дослідження проблеми ідентифікації елементів мікропрограмного управління на основі аналізу процесу електроживлення з метою мінімізації часу виявлення несанкціонованої модифікації параметрів програмно-апаратних засобів (трактів) обчислювальної системи:

модель ідентифікації елемента мікропрограмного управління обчислювальної системи;

метод ідентифікації елемента мікропрограмного управління обчислювальної системи;

метод ідентифікації елементів мікропрограмного управління комунікацією процесів оброблення даних обчислювальної системи;

методика виявлення несанкціонованої модифікації параметрів програмно-апаратних засобів обчислювальної системи на основі аналізу результатів ідентифікації елементів мікропрограмного управління;

методика синтезу автоматизованого комплексу виявлення несанкціонованої модифікації параметрів програмно-апаратних засобів обчислювальної системи.

Висновки. Виявлення несанкціонованої модифікації параметрів програмно-апаратних засобів (множини трактів передавання інформації) обчислювальної системи пропонується здійснювати шляхом співставлення поточних та еталонних результатів ідентифікації елементів мікропрограмного управління на основі аналізу процесів електроживлення при передаванні тестового інформаційного потоку. Практичною складовою наукової роботи є прототип автоматизованого комплексу виявлення несанкціонованої модифікації параметрів програмно-апаратних засобів трактів інформаційних потоків обчислювальної системи.

Ципук О.Р. (ВІТІ)

ПРОГРАМНИЙ МОДУЛЬ АВТОМАТИЗАЦІЇ ОРГАНІЗАЦІЇ НАВЧАЛЬНОГО ПРОЦЕСУ НА ОСНОВІ ЧАТ-БОТУ TELEGRAM

Актуальність**.** Через велике навантаження на курсантів заочної форми навчання виникають проблеми в отримані ними важливої інформації. Це в свою чергу відображається в запізнені чи неприбутті на заняття через незнання чи не отриманні розкладу, витратах значного об'єму зусиль та часу в пошуках потрібної інформації. Але на даний момент технології збору та відображення інформації стрімко розвиваються, виходять все новіші й новіші методи, які дозволяють збільшувати насиченість та зручність отриманої інформації та збільшують її інформативність завдяки використаним технологіям.

Мета дослідження полягає у підвищення ефективності представлення та доступності інформації щодо організації навчального процесу курсантів заочної форми навчання за рахунок виконання наступних часткових завдань дослідження:

– аналіз особливостей організації навчального процесу курсантів заочної форми навчання;

– дослідження особливостей розробки чат-боту підтримки начального процесу;

– автоматизація процесів представлення та доступності інформації щодо організації навчального процесу курсантів заочної форми навчання за рахунок програмного модулю підтримки навчального процесу на основі чат-боту "Telegram".

Виклад основного матеріалу. Використання сучасних технологій в повсякденному житті представляє весь накопичений досвід людства в компактному виді, це призвело до того, що вони проникли у всі сфери, а подібний наслідок має на увазі під собою звільнення людини від потреби отримувати інформацію з багатьох джерел, їх може замінити декілька мобільних чи "десктопних" додатків, їх безліч, тому користувач вибирає саме ті, що потрібні безпосередньо йому. Один з таких Telegram – месенджер, програмне забезпечення для смартфонів, планшетів та ПК, яке дозволяє обмінюватися текстовими повідомленнями та різноманітними файлами, зокрема графічними файлами та відеофайлами, а також безкоштовно телефонувати іншим користувачам програми, та за рахунок ботів існує можливість скоротити використання часу на знаходження чи організацію інформації.

Обліковий запис користувача прив'язується до номеру мобільного телефону: щоб авторизуватися, потрібно ввести код авторизації з SMS. Такі коди мають обмежені терміни придатності. Таким чином, користувач позбавляється необхідності запам'ятовувати чи зберігати десь свій пароль. Для месенджера був створений протокол MTProto, що передбачає використання декількох протоколів шифрування. При авторизації і аутентифікації використовуються алгоритми RSA-2048, DH-2048 для шифрування, при передачі повідомлень протоколу в мережу вони шифруються AES з ключем, відомим клієнту і серверу. Також застосовуються криптографічні хеш-алгоритми SHA-1 і MD5.

Даний програмний модуль має 5 основних клавіш керування ботом. Після його запуску виводить стартове меню. Розділ "Info" надає інформацію про можливості бота. Розділ "Розклад дзвінків" має 2 пункти, користувач обирає, що саме йому потрібно, та після цього натискає на клавішу відповідного розділу. Розділ "Пари" надає інформацію про те, коли починається та закінчується відповідне заняття. Розділ "Сам/по" надає інформацію про часові діапазони годин самостійної підготовки. Розділ "Чергова служба", надсилає користувачу файл з графіком нарядів на інститут. Підказки при введені команд відображаються для більшої зручності в використані бота.

Висновки. Отже, в роботі запропоновано використання програмного додатку, який дозволяє користувачу швидко отримати потрібну йому інформацію, не має: зайвих елементів управління та зайвої інформації. За допомогою програмного модуля курсанту не потрібно знаходити розклад занять, графік дзвінків самостійної підготовки або занять, чи графік чергувань в різних місцях.

Цімура Ю.В. (ВІТІ)
Хоменко П.В. (ВІТІ)
Чуб К.С. (А1906)

ОСОБЛИВОСТІ СУМІСНОЇ РОБОТИ УКХ РАДІОЗАСОБІВ ВИРОБНИЦТВА MOTOTRBO ТА ASELSAN

На сьогоднішній день УКХ радіозв'язок в Збройних силах України організовується з використанням обладнання транкінгового зв'язку „Mototrbo" виробництва компанії „Motorola", яке, в цілому, вирішує завдання забезпечення зв'язку як на стоянці, так і в русі, безпосередньо на полі бою.

Українські військові та інженери компанії Aselsan продовжують реалізовувати спільні проекти, спрямовані на покращення систем зв'язку в Збройних силах України. Одним з таких рішень стало запровадження турецькою компанією у власні засоби зв'язку режиму DMR (DigitalMobileRadio).

В основі технології DMR лежить механізм (TimeDivisionMultipleAccess – багатостанційний доступ з тимчасовим розподілом каналів), що дозволяє розмістити два незалежні канали зв'язку на одній частоті шириною 12,5 кГц і отримати канал з умовною шириною 6.25 кГц.

Режим DMR забезпечує підвищений захист радіомережі від прослуховування. Також він позитивно впливатиме на переоснащення ЗСУ новими радіостанціями, оскільки забезпечує взаємодію підрозділів, оснащених радіостанціями Aselsan з тими підрозділами, що використовують засоби зв'язку Motorola.

Даний режим було впроваджено в радіостанціях Aselsan 9651/9661 для сумісної роботи з існуючим парком радіостанцій Motorola, які широко застосовуються в Збройних Силах України.Сумісність на шифрованих каналах можлива тільки з радіостанціями Motorola, які підтримують алгоритм шифрування AES-256.

Для реалізації зустрічної роботи необхідно виконати наступний алгоритм дій:

встановити програмний продукт AselsanDMRSystemManager (для створення та програмування радіостанцій Aselsan 9651/9661);

встановити програмний продукт MOTOTRBOCustomerProgrammingSoftware (для створення та програмування радіостанцій Motorola);

передбачити налаштування цифрових каналів для зустрічної роботи радіостанцій Aselsan 9651/9661 та Motorola (перелік частот, ключів, розмовних груп);

запрограмувати вищевказані радіозасоби;

На радіостанціях Aselsan 9651/9661 встановити режим роботи DMR та встановити відповідний канал.

Таким чином, радіостанції „Aselsan" в режимі DMR дозволяють забезпечувати взаємодію з радіомережами, побудованими з використанням обладнання „Motorola".

У режимі DMR радіостанція може здійснювати передачі в аналоговому, цифровому нешифрованому або цифровому шифрованому (AES-256) режимі. В нешифрованому режимі аудіо сигнал передається у вигляді відкритого пакету даних, в шифрованому - відповідно у вигляді шифрованого пакету даних.

ЛІТЕРАТУРА

12. Аналіз бойового застосування та характеристик сучасних військових засобів радіозв'язку іноземного виробництва / Гурський Т.Г. // Збірник тез доповідей VII науково-технічної конференції ВІТІ ДУТ. – 2014. – С. 16 – 22.

13. Офіційний сайт компанії „Aselsan" [Ел. ресурс]. – URL: http://aselsan.com.tr.

д.в.н. Чабаненко П.П. (ЦНДІ ОВТ ЗСУ)
к.т.н. Розгонаєв С.М. (ЦНДІ ОВТ ЗСУ)
Бігун Н.С. (ЦНДІ ОВТ ЗСУ)

НАВЧАННЯ ОПЕРАТОРІВ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ УПРАВЛЯЮЧИХ СИСТЕМ

Актуальність, постановка задачі. На ефективність високоінтегрованої системи управління в сфері безпеки і оборони (СБО) країни великий вплив має підготовленість її операторів. Відомі різні моделі навчання людини, серед яких змістовні та при цьому дають кількісну оцінку навченості моделі Р. Аткінсона, які він використовував для дослідження психофізіологічної основи пам'яті людини. Стосовно до інтегрованої системи СБО динаміка навченості операторів (колективу, бойової обслуги, персоналу) має бути викладена в природних показниках, адекватних функціях, завданнях і цілях СБО. До таких показників відносяться ймовірності безпомилкового та своєчасного їх виконання на відповідному кроці навчання.

Мета. Апробація методу формалізованого навчання операторів (персоналу, бойової обслуги) інтегрованих систем.

Основні положення. Крок навчання - цілісний типовий фрагмент цілеспрямованого процесу, який здійснюється в циклі навчання. Змістовне його наповнення може бути різним, але близьким за складністю. Передбачається можливість обмеження на час його виконання і постановка в відповідність мети події «правильний результат». Підготовка навчання операторів включає розділення процесу його діяльності за рішенням навчального завдання на покрокові фрагменти і забезпечення реєстрації результатів їх виконання в тренажерному режимі реальної системи або в навчальному кабінеті.

Моделювання динаміки навчання здійснюється на основі математичного апарату зворотніх (рекурентних) послідовностей. При цьому процес навчання розглядається як формування у операторів необхідних розумових моделей дій для ефективної діяльності в реальних умовах. Особливість сполучення необхідності обліку істотних залежностей в процесі навчання за часів незалежності кроків в математичному методі полягає в тому, що залежності враховуються в межах однокрокової моделі процесу. Циклічність навчання утворюється зворотним зв'язком, по якому результат кожного кроку звертається в початкові умови наступного кроку. Зміни стану навчаємого оператора (бойової обслуги) розглядається в просторі координат, співвіднесеному цілі дослідження. Враховуються: поліпшення, збереження або погіршення його стану.

Детальний виклад запропонованого загальнонаукового методу дано автором у книзі «Дослідження безпеки та ефективності функціонування систем людина-техніка ергомережами» (2012 р., 160 с., с. 123-154) з додатком та розрахунками траєкторій освоєння ефективних управлінських функцій. Розроблений метод удосконалений для обліку перенавчання, освоєння суміжної спеціальності.

Висновок. Застосування методу ефективне при дослідженні таких систем, ефективність яких залежить як від досконалості техніки, так і від організації процесу функціонування з урахуванням людського фактору. Можливість безпомилкових, помилкових і аварійно-небезпечних результатів враховується в природних (об’єктивних) показниках.

Представляється продуктивним коректне застосування рекомендованого методу формалізації навчання систем людина-техніка спільно з інтуїцією і професійним досвідом педагогів навчальних закладів та керівників бойової підготовки військових підрозділів в інтегрованих системах. Досвід показує, що однієї творчої складової, що не підкріплена чисельним методом оцінювання, для досягнення значущого дидактичного ефекту недостатньо.

д.т.н. Чевардін В.Є. (ВІТІ)
Пономарьов О.А. (ВІТІ)
Штобза Д.В. (ВІТІ)

НОВІ ПАРАМЕТРИ ЕЛІПТИЧНИХ КРИВИХ ДЛЯ КРИПТОГРАФІЧНИХ ДОДАТКІВ

Актуальність. В основі більшості сучасних програмних додатків, які використовуються для послуг забезпечення цілісності, причетності та безвідмовності користувачів в комп'ютерній мережі лежать методи скалярного множення точок еліптичної кривої.

Це основна та найбільш складна сучасна криптографічна операція, яка використовуються в алгоритмах генерації та верифікації цифрового підпису ECDSA , генерації асиметричних ключів шифрування та інших криптографічних алгоритмах.

В зв'язку з цим, за останні двадцять років з'явилося багато стандартів, які використовують арифметику еліптичних кривих, а саме IEEE P1363, FIPS 186-3 (Digital Signature Standard), в яких рекомендованы криві використовують криві вида: y2 = x3 +Ax +B mod p, які реалізовані в різних бібліотеках IEEE 1363 Dynamic Link Library, , з яких найбільшою увагою користується бібліотека Miracl. Це криві: ssc-160, ssc-192, ssc-224, ssc-256, ssc-288, ssc-320, ssc-384, ssc-512.

Але враховуючи існуючі тенденції збільшення потужності квантових комп'ютерів постає питання вдосконалення існуючих алгоритмів, які використовують операції в групі точок еліптичної кривої на перехідний період.

В зв'язку з чим, **метою** роботи є розробка нових параметрів еліптичних кривих, які забезпечать підвищення криптографічної стійкості існуючих програмних та програмно-апаратних додатків.

Основна частина. Під час проведення досліджень були розроблені програмні додатки для генерації еліптичних кривих на основі бібліотеки програмних функцій Miracl, а саме був використаний додаток для генерації поліномів schoof2, алгоритм генерації кривої та перевірки параметрів безпеки кривої sea, алгоритм генерації поліномів по модулю простого числа modmull.

Результати генерації нових параметрів кривих були представлені для кривих у формі Вейерштрасса $y^2 = x^2 + Ax+B(\text{mod } p)$ та еквівалентних скручених кривих Едвардса в інверсній формі: $x^2 + 2y^2= x^2 y^2+ d(\text{mod } p)$.

Під час генерації криві були перевірені на стійкість до MOV атаки з коефіцієнтом к = 50.

В ході досліджень були отримані нові параметри кривих та представлені в наступному вигляді.

Крива над полем з довжиною характеристики p - 256 бітов

	dec	hex
p	115792089237316195423570985008687907853269984665640564039457584007913129639013	ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffc65
n	28948022309329048855892746252171976963357524003033751936551228399944822236563	40000000000000000000000000000001E1D14B6ED53005C107434A962152593
d	107	6B
A	17774219124880787590524118104869352860007719008923671202669751431476954123589	274BD9FD0448F3568702F21F24869C50C389805871ABF4DFCC485EDA0279CD45
B	38803163055334738429996826000694465650850577966436874629690975997838100814535	55C9CFDEB5B1DD9145E88D5A416D3BCE364111DF55250082AE827EDC4E345AC7

Криві над полем з довжиною характеристики р - 512 біт

	dec	hex
p	134078079299425970995740249982058461274793658 205923933777235614437217640300735469768018742 981669034276900318581864860508537538828119465 6994643364900608 3221	fffffffffffffffffffffffffffffffffffffffffffffffffff fffffffffffffffffffffffffffffffffffffffffffffffffff fffffffffffffffffffffffc95
n	335195198248564927489350624955146153186984145 514809834443089036093044100751840512613445736 220066515147934100158598747475094307363660134 1402240469528982943	400000000000000000000000000000 000000000000000000000000000000 000028A3CE52209E2BD4952882D557 4165192C46C0D0311FEA6BF9FECE70 EE63B59F
d	269	10D
A	162165883004146492429701778636530076864991298 985694816313703004864897270959184937868075202 639906387108338191722771126861976231483526249 6015896738277047332	1EF680D4C3CE5C69ABD1D21042CE1 D23F92E9AAC6D296239C08C23372B 19F3F101B8CFD6B19382912F6B5A7A B7F98F1D46D5A022FBA6B403AB685 F0F2A973C24
B	447332529417627074254769691065488964789114886 113817530853940527841360353986096783984660522 745743628062839127684157584023137314696139024 371693164131868 8583	556928981DB52657124C5282DBB662 6BF5B6DCFAC789CD4428112402669 C9D2E99F22869E9F7AD96473859F58 2F9138DC4E741444244FEF092D8269 B7DB5C747

Висновок. Під час проведення досліджень використовувались криптографічні функції та алгоритми, реалізовані в бібліотеці програмних функцій з наступними параметрами. В якості показника безпеки використовувалась характеристика скінченного поля над яким побудована крива. Криві подаються двома коефіцієнтами *a* = 2, *d* – найменший квадратичний невід'ємник, $\left(\frac{d}{p}\right) = -1$ для характеристики поля р. Для кожній кривій розраховано порядок циклічної *n* підгрупи точок скрученої кривої Едвардса в інверсних координатах. Для кожній згенерованої кривої розраховані коефіцієнти А та В еквівалентної кривої Веєрштраса. Отримані криві перевірені на стійкість до MOV атаки на предмет відповідності вимогам стандарту IEEE P1363 з безпеки криптографічних додатків на еліптичних кривих. Для визначених параметрів та побудованої кривої були згенеровані випадкові точки порядка *NP/4,* де *NP* – порядок групи точок кривої Едвардса. Усі точки перевірені скалярним множенням на число *NP/4* з обґрунтуванням щодо можливості їх використання в криптографічних додатках.

Отримані нові параметри еліптичних кривих в формі Веєрштраса та формі Едвардса дозволяють підвищити рівень стійкості сучасних алгоритмів ЕЦП на основі кривих на простими полями з характеристикою довжиною 512 біт. Зроблені оптимізації та налаштування програмних додатків на основі бібліотеки Miracl дали змогу отримувати нові параметри підвищеною стійкості для еліптичних кривих. Це відкриває додаткові шляхи вдосконалення існуючих стандартів криптографічного захисту інформації, а саме ЕЦП на перехідному періоді до переходу на нові стандарти постквантової криптографії.

Майбутні дослідження будуть присвячені генерації еліптичних кривих та параметрів для криптосистем над полями характеристики довжиною 768 та 896 біт.

Чередніков С. О. ПП „Компанія Крокус-Ком”

ТЕНДЕНЦІЇ РОЗВИТКУ ЗАСОБІВ ЗВ’ЯЗКУ ТА АВТОМАТИЗАЦІЇ НА ПРИКЛАДІ ЗАСТОСУВАННЯ ГІБРИДНИХ (IP-TDM) СИСТЕМ ДИСПЕТЧЕРСЬКОГО ТА КОНФЕРЕНЦ-ЗВ’ЯЗКУ ТА АВТОМАТИЗОВАНИХ СИСТЕМ РАДІОРЕЛЕЙНОГО ЗВ’ЯЗКУ

Сучасний стан та тенденції розвитку технологій зв’язку знаходяться на перехідному періоді одночасного застосування частотних , TDM та Ethernet технологій тобто гібридного стану телекомунікаційної мережі. Кожна з цих технологій має свої переваги та вади і має право на існування в єдиній глобальній системі комунікацій. Однією з пріоритетних тем для організації системи підтримки прийняття рішень спеціального призначення та бойового застосування зв’язку є організація диспетчерського та конференц зв’язку (в тому складі і гучномовного) в рамках існуючої гибридної телекомунікаційної мережі. Використання для цього технології ASTERISK не дозоляє забезпечити якісну мережеву структуру селекторного та конференц зв’язку із-за потреби великого обчислювального ресурсу системи обробки викликів та нестабільністю її роботи. ПП „Компанія Крокус-Ком” пропонує оригінальну технологію роздільної організації мережі зв’язку, а саме лишити IP транспортний рівень без змін, а рівень обробки інформації. комутації, мікшерування та авто вирівнювання по гучності перенести на рівень обробки в TDM технології. Переваги – значно скорочується трафік службової інформації, нема потреби в великих обчислювальних ресурсах абонентських термінальних та базових складових системи конференц та селектороного зв’язку. Запропоновано базовий модуль в 60 абонентів зв’язку в єдиному пристрої. Децентралізована система об’єднання даних базових модулів в IP мережі дозволяє побудувати єдину мережеву структуру IP конференц та селекторного аудіо зв’язку зі значною кількістю його учасників (теоретично за 1000) з значно кращими якісними характеристиками, що не можливо при застосуванні технології ASTERISK. Запропонована **система СПРУТ- К** – унікальна система і на сьогодні єдина, що призначена для організації аудіо селекторного та конференц зв`язку абонентів IP телефонії та гучномовного зв’язку без використання технології ASTERISK. Конференції проходять як по „кабінетному” принципу, так і по вибраному контенту. Система має внутрішній SIP сервер на 256 транків так і може використовувати зовнішній SIP сервер з 256 напрямків SIP серверів . Візуалізація настроювання й керування конференціями здійснюється з ПЭВМ як з місця установки системи, так і дистанційно по WEB інтерфейсу.

Особливості системи:

IP конференція – всього 60 абонентів, кількість кабінетів макс.– 6, максимально в кабінеті – 60 абонентів.

Диспетчерський (селекторний) зв’язок – максимально 29 абонентів з використанням пульта ГЛАС-Д. Можлива сумісна робота з режимом Конференції.

Протоколи: SIP-RFC3261,3262,3263,3264, 3265,3515,2976,3311, SDP-RFC 2327, RTP / RTCP-RFC2198, 1889.

Мережеві протоколи IP, TCP, UDP, TFTP, FTP, RTP, RTCP, ARP / RARP, ICMP Ping, NTP, NTP, Http.

Параметр конфігурации SIP клиєнтів DTMF: SIGNAL/RFC283/INBAND;

DNS Кодеки: G.711A/U law(V.17, V.21, V.27ter, V.29), G.723.1, G.729A/B/E, G.726 (40/32/24/16), AMR,ilbc;

WEB інтерфейс з україномовним монітором.

Досвід експлуатації в ЗСУ – 1 рік.

Крім того ПП „Компанія Крокус – Ком” розробила та пропонує:

Універсальний комплекс гучномовного зв’язку (УКГС) „ГЛАС” призначений для організації гучномовного зв’язку з абонентами по 2 чи 4 проводових фізичних лініях з реалізацією циркулярного, селекторного та конференц зв’язку, як з місцевим, так і з дистанційним електроживленням абонентських теріналів і одночасного використання IP абонентських виносів.

Застосування – системи зв’язку ППО, військових частин, базових та польових формувань, систем охорони військових об’єктів та керуючих органів ЗСУ і силових структур. Режими роботи:

1. „Кінцевий” – обладнання використовується в якості кінцевого гучномовного обладнання 2 проводового каналу.

2. „Циркуляр” – всі абонентські пристрої приєднуються до однієї двухпроводной лінії (максимум 30 обладнань) і забезпечують зв’язок „усі чують всіх з правом одночасної розмови”.

3. „Диспетчер” – з’єднання „зірка”, де диспетчер з пультом (1) та абоненти (29) з'єднані кожний по окремій парі фізичного кабелю.

Загальні технічні характеристики: максимальна кількість каналів: 30;

рівні приймання/передачі каналів абонентів: 0 дб / – 7 дб;+4,3 дб / – 13 дб; переходное загасання між будь-якими каналами на частоті 800 Гц < ’ 60 дб; нерівномірність АЧХ розмовних каналів у смузі частот 300 Гц … 3,4 кГц ’ 1,9 дб; максимальная довжина абонентського виносу по фізичному кабелю – 3 км., (включно з дистанційним живленням) ; Джерело живлення = 12 В;~220 в. Досвід експлуатації в ЗСУ– 3 роки.

Цифрова мультисервісна автоматизована радіорелейна система TRANSCEND 800B – система нового покоління розроблена для Замовника: ВСУ, силових відомств, мобільних операторів зв’язку й підприємств. Унікальність її насамперед полягає в можливості стійкого тримання зв’язку в самих радіозашумлених та закритих інтервалах РРЛ, де інші системи РРЛ та ШПД просто не працюють. І це завдяки наявності узкополосних режимів модуляції з полосою від 1,75 до 7 Мгц і далі до 56 Мгц. та унікальному сумісному протоколу виправлення помилок LDPC+BCH де сигнал може бути виділений на 0.6– 1.2 дБ нижче теоретичної границі Шеннона, а також наявності автоматизованого комплексу самонаведення та адаптаціїї до геофізичних умов. Система не має аналогів в Україні та орієнтована на :

1. Гибридність організації трафіку Ethernet, IP, і TDM технологій до 400 Мбіт,

2. Комплексність рішення зв’язку: В одному комплексі ЦРРС+ Гбит Комутатор L2+Гбит маршрутизатор L3+ Система орієнтації та самонаведення + IP Sec 256+Комплекс керування й моніторингу. (84E1,400Mb Ethernet,2xSTM1.

Основні технічні характеристики:

Частота: Transcend 800 працює діапазонах частот від 4,4 ГГц до 38 ГГц.

Види модуляції: QPSK, 8PSK, 16QAM, 32QAM, 64QAM, 128QAM і 256QAM, причому в кожному з них реалізовано від 2 до 5 їх різновидів по відносній швидкості кодування 1/2, 3/4, 5/6, 7/8, 10/11, що вкрай важливо для роботи в зашумленому просторі.

Смуга частот модуляції: від 1,75 МГц до 56 МГц, Особливо корисний узкосмуговий сигнал;

Максимальна пропускна здатність: Eth-400 Мбит/з, 84 хЕ1, 2х STM–1, прямий DVB-ASI , що „з головою” хватає вирішувати всі проблеми ЗСУ;

Система має вбудований комутатор L2:4 х портовий (10/100/1000Baset Ethernet) з підтримкою VLAN, Q – in – Q, Jumbo frame 9k.

Система має вбудований маршрутизатор L3: 3-х портовий (3 х 10/100/1000Baset IP) з підтримкою розширеної Qos і MPLS; технологія прямої DVB – ASI інкапсуляції в радіоканал; Адаптивна модуляція й кодування: ACM; Завадостійке кодування: LDPC+FEC ,що забезпечує пропускну здатність 0.6–0,8 дБ нижче теоретичної границі Шеннона); Агрегація трафіка: від 1+0,1+1 до 12+0;

Безпека доступу: 4 рівня пріоритетів для доступу до мережного елемента (http/cli) + IP SEC (ключ 256); Вбудована системв самонаведення: автоматична система визначення координати й самонаведення на другу сторону РРЛ; Довжина рознесення модем (IDU) – приймач-передавач (ODU)- 300 м.(унікальний діапазон); Температурний діапазон: – 35С + 60С внешн. -5С + 50С внутр. Досвід експлуатації в ЗСУ – 4 роки. Система постійно модернізується .

Черноног О.О. (ГУЗІС ГШ ЗСУ)
Жовтун А.А. (НЦЗІ ВІТІ)
Терещенко Т.П.(НЦЗІ ВІТІ)
к.т.н. Козубцов І.М. (НЦЗІ ВІТІ)

ВИБІР АВТОМОБІЛЬНОЇ ПЛАТФОРМИ ВИСОКОЇ ПРОХІДНОСТІ ДЛЯ ПІДРОЗДІЛІВ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ЗБРОЙНИХ СИЛ

Постановка завдання. З появою нових підрозділів кібернетичної безпеки вбачається за необхідність вирішення питання щодо її оснащення матеріально-технічними засобами – мобільними апаратними.

Сьогодні основу автомобільного парку Збройних Сил (ЗС) складає технічно застаріла автомобільна техніка марок КрАЗ, Урал, ЗіЛ, ГАЗ, КамАЗ, МАЗ, УАЗ різних модифікацій, розроблених в 40-60 роках. Перераховані автомобілі, за винятком КрАЗів, зроблені за межами країни – в Росії та Білорусії.

Враховуючи сучасний фінансово-економічний стан нашої держави, закупівля апаратних іноземного виробництва з економічної точки зору є цілком неприйнятною, оскільки це значно збільшує кошти і матеріальні витрати на їх експлуатацію, технічне обслуговування, постачання запасних частин та способи їхнього відновлення у військах, так і на заводах з капітального ремонту. Тому, метою доповіді є обґрунтування вибору автомобільну платформу високої прохідності для забезпечення функціонування підрозділів кібернетичної безпеки ЗС.

Результат дослідження. На першому етапі дослідження вивчалися вимоги, які висуваються до апаратних військового призначення з урахуванням рекомендації одержаних в процесі військових навчань щодо ергономіки.

На другому етапі формували критерії вибору, а саме: замкнутий технологічний цикл виробництва автомобілів високої прохідності в Україні; вартість відвантаженої одиниці виробу; висока прохідність; надійність і простота технічного обслуговування автомобілів.

На третьому етапі вивчалися вітчизняні виробничі можливості підприємств автомобілів високої прохідності із врахуванням задоволенням виконання вимог сформованих на другому етапі (табл. 1).

Таблиця 1

Виробничі можливості українських виробників автомобільної платформи

№ п/п	Найменування виробника	Автомобільна платформа	Замкненість процесу		
			Автомобільна платформа	КУНГ	Причеп
1	ПАТ „НАФТОАВТОМАТИКА”	КрАЗ	-	+	-
2	ТОВ НВП ТОПАЗ-М	КрАЗ	-	+	+
3	ТОВ „ІНТЕРКАРГОТРАК”	КрАЗ	-	+	
	ПАТ „АвтоКрАЗ”.	КрАЗ	+	+	+
	НВП „Практика”	КрАЗ	-	+	+

Переліченим вимогам до автомобільної платформи задовольнила КрАЗ. А щодо забезпечення замкнутого технологічного циклу виробництва забезпечено лише в ПАТ „АвтоКрАЗ”.

Таким чином, раціональним для створення вітчизняних апаратних кібернетичної безпеки є використання виробничої бази КрАЗ автомобільного заводу ПАТ „АвтоКрАЗ”, який наданий час виступає єдиним українським виробником важких вантажних автомобілів із замкнутим технологічним циклом виробництва.

Черноног О.О. (ГУЗІС ГШ ЗСУ)
Куцаєв В.В. (НЦЗІ ВІТІ)
Козубцова Л.М. (ВІТІ)
к.т.н. Козубцов І.М. (НЦЗІ ВІТІ)

ПОНЯТТЯ ТЕРМІНУ ГЛОБАЛЬНОГО КОЛАПСУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Постановка завдання. При відпрацюванні проекту попереднього опису майбутнього безпекового середовища „Майбутнє безпекове середовище 2030. „Чорні лебеді 2030 (стратегічний шок)" перед особовим складом науково-дослідним відділом кібернетичної безпеки в інформаційно-телекомунікаційних системах (ІТС) і виникла стояла задача обґрунтувати нове поняття „Глобальний колапс ІТС".

Мета доповіді є апробувати запропонований зміст поняття терміну "глобальний колапс ІТС".

Результат дослідження. Поняття терміну „Глобальний колапс ІТС", в процесі відпрацювання проекту попереднього опису майбутнього безпекового середовища виявилось новим, оскільки в енциклопедичних словниках та у відкритих джерелах воно відсутнє. Натомість широко набули вжитку такі терміни як „економічний колапс", "екологічний колапс", „фінансовий колапс" „політичний колапс", „соціальний колапс", та ін. Зважаючи на повномасштабне впровадження у повсякденну діяльність електронних інформаційних технологій на інтуїтивно відчувається необхідність терміну "Глобальний колапс ІТС". Так у разі снігових бур, від звичайного обезструмлення та інших форс-мажорних обставин приховує колосальні наслідки від порушення роботи ІТС.

Наслідки воєнного характеру можуть настати в разі збою та несанкціонованого керування військами та озброєнням до прикладу, як у фантастичному фільмі „Terminator", де штучний інтелект мережі „SkyNet" отримавши доступ до керування системою протиракетною оборони та ядерним озброєнням Збройних сил США створив умови до знищення людства. І хоча на перший погляд це виглядає фантастично, але сьогоднішні "кібервійни" та "кіберпростір" з науково-фантастичного роману У. Гибсона „Нейромант" (1982 р.) перекочували в сучасну реальність.

Виходячи з розглянутих передумов синтезуємо систему понять нового терміну „Глобальний колапс інформаційно-телекомунікаційних систем", що містить складові: „глобальний" + „колапс" + „інформаційно-телекомунікаційні системи". Розглянемо змістовне наповнення кожного терміну окремо, а згодом їх об'єднаємо:

„глобальний" – який стосується всієї земної кулі, всього людства; всесвітній;

„колапс" – процес руйнування будь-якої структури під впливом системного кризису;

„інформаційно-телекомунікаційна система" – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Таким чином, пропонуємо термін поняття "глобальний колапс інформаційно-телекомунікаційних систем", трактувати як настання глобальних наслідків планетарного значення техногенного, технологічного, економічного або військового характеру в наслідок деструктивного кібернетичного впливу, націленого на руйнування технологічних процесів (алгоритмів) нормального функціонування інформаційно-телекомунікаційної системи (сукупності інформаційних та телекомунікаційних систем) та мережі, в результаті чого порушується інформаційна безпека, а саме здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації.

Наукова новизна. На підставі системних збоїв які існують в ІТС обґрунтовано та введено у обіг нове поняття терміну "глобальний колапс інформаційно-телекомунікаційних систем".

к.т.н. Чумак В.К. (ВІТІ)
к.т.н. Шишацький А.В. (ЦНДІ ОВТ)
к.т.н. Борисов О.В. (ВІТІ)

МЕТОДИКА УПРАВЛІННЯ ПАРАМЕТРАМИ БАГАТОАНТЕННИХ СИСТЕМ ІЗ ШУМОПОДІБНИМИ СИГНАЛАМИ

Сучасні військові системи радіозв'язку (ВСРЗ) функціонують в складній радіоелектронній обстановці,що характеризується наявністю в каналі зв'язку навмисних завад та завмирань сигналу. Однією з технологій,що дозволяють ефективно боротися з навмисними завадами та завмираннями сигналу, а також значно збільшити перепускну здатність радіоканалів є технологія „багато входів – багато виходів" (MIMO – *Multiple-InputMultiple-Output*) У технології MIMO об'єднані просторово-часові методи прийому з використанням адаптивних антен і методи просторово- часового кодування і просторово-часового розділення сигналів. Іншим напрямком підвищення ефективності ВСРЗ є надширокосмугові сигнали (UWB – *Ultra wideband*). Надширокосмугові сигнали (НШСС) мають високу завадозахищеність, можливість адаптивного управління параметрами, низький (шумоподібний) рівень сигналу, забезпечує ефективне використання радіочастотного ресурсу.

Важливим напрямком при вирішенні задачі підвищення ефективності ВСРЗ є створення гібридних інформаційних технологій, що дозволяє об'єднати переваги традиційних технологій та зменшити їх недоліки.

В роботі запропонована методика управління параметрами багатоантенних систем з шумоподібними сигналами, яка складається з наступних етапів.

1. Введення вихідних даних. Вводяться параметри передавального пристрою і каналу зв'язку, а також значення допустимої величини ймовірності помилкового приймання сигналів та мінімально необхідної швидкості передачі інформації.

2. Оцінка стану каналу зв'язку. За допомогою відомих методів оцінки стану каналу зв'язку проводиться оцінювання стану каналу зв'язку.

3. Вибір робочих частот з урахуванням стратегії засобів радіоелектронного подавлення. Проводиться аналіз радіоелектронної обстановки в діапазоні робочих частот, під час якого здійснюється визначення подавлених частотних діапазонів та стратегії комплексів радіоелектронного подавлення.

4. Прогнозування стану каналу зв'язку. В лінійному тракті прийомопередавача засобу радіозв'язку (ЗРЗ) виділяється смуга субчастот, що розміщені біля однієї фіксованої частоти. По всій смузі частот здійснюється підтримання сталого рівня сигналу за допомогою цифрової системи автоматичного регулювання потужності передавача. Цифровий синтезатор частот формує сітку сигналів, що надходить на демодулятор. Основною задачею статистичного аналізу випадкових полів спостереження є побудова полів та вибір номерів, субчастот, в яких рівні завад, та ймовірності бітових помилок будуть мінімальні. Отриманні номери субчастот надходять на блок управління.

5. Визначення кількості антен у системі MIMO. На зазначеному етапі в залежності від стану каналу зв'язку обирається, ,кількість передавальних та приймальних антен для ЗРЗ з урахуванням необхідного відношення сигнал/шум та необхідної швидкості передачі.

6. Вибір параметрів НШСС. На зазначеному етапі відбувається створення формуючого поліному, який в залежності від сигнально-завадової обстановки формує оптимальні параметри НШСС.

Новизна розробленої методики полягає у виборі робочих частот з урахуванням стратегії комплексів радіоелектронного подавлення та прогнозуванні стану каналів зв'язку, а також адаптації параметрів гібридної MIMO-UWB системи дозволяє підвищити ефективності функціонування військових систем радіозв'язку.

к.т.н. Шаповалов О.В. (ХНУПС)

МЕТОДИ ФОРМУВАННЯ ОЗНАК ПРИ ПОВЕДІНКОВОМУ АНАЛІЗІ ТРАФІКА КОНВЕРГЕНТНИХ МЕРЕЖ

Актуальність, постановка задачі. Системи виявлення вторгнень (Intrusion-Detection Systems – IDS) та запобігання їм (Intrusion-Prevention Systems – IPS) на даний час є необхідним знаряддям забезпечення надійного кіберзахисту інформаційно-телекомунікаційних систем військового призначення. IPS можна класифікувати за наступними категоріями:

– Мережеві IPS (Network-based Intrusion Prevention, NIPS): відстежують трафік в комп'ютерній мережі і блокують підозрілі потоки даних.

– IPS для бездротових мереж (Wireless Intrusion Prevention Systems, WIPS): перевіряє активність в бездротових мережах. Зокрема, виявляє неправильно налаштовані точки бездротового доступу до мережі, атаки людина посередині, спуфінг mac-адрес.

– Аналізатор поведінки мережі (Network Behavior Analysis, NBA): аналізує мережевий трафік, ідентифікує нетипові потоки, наприклад DoS і DDoS атаки.

– IPS для окремих комп'ютерів (Host-based Intrusion Prevention, HIPS): резидентні програми, що виявляють підозрілу активність на комп'ютері.

Однак, слід зазначити наявність вагомого недоліку, який знижує ефективність IDS та IPS в умовах швидкоплинної зміни загроз у кіберпросторі – в своїй роботі зазначені системи спираються головним чином на статичні сигнатури.

Мета. Розробка методів, що дозволяють системам IDS і IPS ідентифікувати підозрілий трафік, навіть якщо вони раніше і не стикалися зі зразками подібного трафіка, породженого несанкціонованими діями являє собою значний інтерес.

Одними з підходів є використання евристичних і поведінкових методів аналізу, які дають можливість виявляти файли і процеси, що містять ознаки потенційної загрози.

Основні положення. Розглядаючи трафік в комп'ютерній мережі як випадковий процес, поняття „форма" процесу розглядається як лінгвістична характеристика, яка побічно визначає залежність його елементів, може бути формалізована (представлена чисельної мірою) і здатна бути використана у подальшому формуванні простору ознак.

Пропонується вирішувати завдання оцінки параметрів (розкриття структури) хаотичного відображення по сформованому з його допомогою сигналу, спираючись на властивості BDS-статистики. BDS-статистика і побудована на її основі відносно нова процедура – BDS-тест були запропоновані в результаті аналізу фінансових ринків економістами Броком, Дечерт і Шейнкману (B. Brock, W. Dechert і J. Scheinkman) в 1987 і представляють один з потужних методів виявлення залежностей у часових рядах, інтенсивно розробляються в останнє десятиліття в рамках їх нелінійного аналізу.

Його мета полягає в тому, щоб розрізнити дані I.I.D. (independent and identically distributed) і будь-який вид залежності – перевірити нульову гіпотезу про незалежність і тотожний розподіл значень часового ряду, використовуючи для цього критерій значущості.

Висновок.

Авторами розглянуто існуючі методи поведінкового аналізу та запропоновано метод формування ознак трафіка в конвергентній мережі.

Проведено аналіз та порівняння параметричних та непараметричних методів.

Швець Ю.О. (ВІТІ)
Троцько О.О. (ВІТІ)

АСУ ТЕХНОЛОГІЧИМ ПРОЦЕСОМ SCADA-SYSTEM В ЗАСТОСУВАННІ ІНТЕЛЕКТУАЛІЗАЦІЇ ПРОЕКТУВАННЯ ТЕХНОЛОГІЧНОГО ПРОЦЕСУ ПІДПРИЄМСТВ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ

В ході останніх кібернавчань НАТО стало відомо, що основним кіберпідрозділам Північноатлантичного Альянсу вже не такі цікаві пристрої на Android або веб-камери: фокус уваги військових хакерів змістився в бік систем Windows і Supervisory Control And Data Acquisition (SCADA).

SCADA – це програмно-апаратний комплекс, призначений для розробки або забезпечення роботи систем збору, обробки, відображення та архівування інформації про об'єкт моніторингу або управління. SCADA-системи дозволяють розробляти автоматизовані системи в розподіленій, як правило, клієнт-серверній архітектурі. Досліджуючи можливості застосування складних SCADA-систем на підприємствах Міністерства оборони України, варто зазначити, що більшість SCADA-систем працює під управлінням ОС Windows в режимі реального часу.

Основними складовими SCADA-систем є диспетчерський пункт управління (автоматизоване робоче місце), підсистема отримання та архівування інформації (сервер), комунікаційні засоби (мережеві протоколи, інтерфейси обміну даними). Будь-який з цих елементів може бути підданий атаці зловмисника і, відповідно, повинен бути захищений. Однак питання інформаційної безпеки сучасних SCADA-систем все ще недостатньо опрацьовані, тому дослідження у цій сфері є актуальними.

Одним з варіантів вирішення розглянутих проблем пропонується захист від неправильних дій SCADA-системи, що зазнала атаки зловмисника, на рівні контролерів управління.

Беручи до уваги те, що людина-диспетчер може знаходитись в умовах невизначеності та жорсткого дефіциту часу, функція інтелектуалізації SCADA-систем повинна включати, крім традиційного ситуаційного і логічний аналіз подій і стану, прогнозувати поведінку технологічного процесу і оперативний пошук дій при виникненні нештатних ситуацій.

Будь-яка експертна система включає в себе основні блоки: підсистема логічного висновку, яка використовує інформацію з бази знань (БЗ), генерує рекомендації щодо вирішення шуканого завдання; модулі відображення; модулі пояснення рішень.

А основними категоріями вирішуваних завдань є: діагностика, управління (в тому числі технологічним процесом), інтерпретація, прогнозування, проектування, налагодження і ремонт, планування, спостереження (моніторинг), навчання.

Таким чином, інтелектуалізація традиційних SCADA-систем шляхом застосування експертної системи – один з головних шляхів розвитку засобів штучного інтелекту.

Створення експертної системи може значно прискорити процес проектування складної системи управління технологічним процесом, підвищити якість виконання завдання і дати економію ресурсів за рахунок ефективного розподілення функцій центрального управління і локальних вимірювальних і управляючих підсистем. Такий ефект досягається за рахунок відкритості системи подання знань про об'єкт управління, адаптування системи до умов функціонування, автоматичної корекції керуючої результатом при зміні істотних параметрів в процесі функціонування.

ЛІТЕРАТУРА

1. Тарасов В. Б. Інтелектуальні SCADA- системи: витоки і перспективи / В. Б. Тарасов, М. Н. Святкіна // Наука і освіта. Електрон. журн. МГТУ ім. Н. Е. Баумана. 2011. № 10.

2. Самойлова Е. М. Проектування системи автоматизації на основі застосування SCADA-системи / Е. М. Самойлова, А. Н. Колябіна // Автоматизація та управління в машино- і приборостр-ванні: зб. науч. тр. Саратов: СГТУ, 2011. З. 196 – 201.

Шейгас В. В. (ЖВІ)

СПОСОБИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ БЕЗПІЛОТНИМ ЛІТАЛЬНИМ АПАРАТАМ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

На даний час одним з видів оптичної (видової) розвідки є застосування безпілотних літаючих апаратів.

При тому що час на підготовку оператора (пілота) найпростішого безпілотного літаючого апарату, з можливістю передачі відео інформації не перевищує кількох годин, протидія даним апаратам стає все важчою, зважаючи на розвиток методів та засобів приховування факту передачі інформації.

Затребуваність заходів протидії безпілотним літаючим апаратам, в тому числі і цивільним, обумовлена високим числом інцидентів з літаючими дронами, можливістю їх застосування для вбивств, терактів та інших протиправних дій.

Проблема більшості сучасних рішень - висока вартість і виникнення небезпеки для людей і об'єктів, що знаходяться в точках, куди можуть звалюватися некеровані або виведених з ладу безпілотники або їх частини.

При аналізі методів та засобів протидіїї різними країнами застосовувались різні рішення.

Акустичні. Акустичний удар викликає резонанс механічної частини бортового гіроскопа. Застосовується з 2015 року.

Лазерні. У 2015 в Німеччині розроблено власну лазерну систему, здатну збивати БпЛА на відстанях до 5 км.

З 2015 року США застосовує малопотужні лазери, здатні збивати дрони.

З 2017 року Китай експортує лазерні установки для боротьби з малими безпілотниками, установка здатна знищити наземну або повітряну ціль розміром з безпілотник з відстані близько 4 км.

Мікрохвильові. Використовують для дистанційного „підсмажування" електроніки дрона, наприклад, спрямованим СВЧ випромінюванням.

З 2016 коку США застосовує комплекс з СВЧ випромінюванням, заявлено що він спроможний збити цілий рій безпілотників.

Протидрони. Застосовуються дрони, оснащені більш потужними двигунами, наприклад, дизельними, з більш захищеним корпусом і пристроями для руйнування інших дронів, наприклад, незаконно запущених або на заборонених для польотів територіях. Дрони-перехоплювачі автоматично наводяться, наприклад, по шуму двигунів переслідуваного дрона або по його зображенню в системі „комп'ютерного зору" дрона-перехоплювача.

З 2015 року у Токіо застосовують більш потужні дрони, забезпечені сіткою, які мають вилітати на перехоплення хобі-дронів, які перебуватимуть там, де їм бути не належить.

У 2016 році у США розроблено систему для вилову безпілотників з більш потужного БЛА, забезпеченого кевларовою сіткою.

Радіоелектрона боротьба. Можна виділити наступні види дії РЕБ:

– системи автоматичного виявлення безпілотника в заданому секторі (оптичні, радарні, акустичні, по-радіовипромінюванню, комбіновані);

– системи перехоплення управління безпілотником;

– системи постановки перешкод в каналі управління безпілотником;

– системи постановки перешкод для роботи систем геопозиціонування БпЛА на частотах систем супутникового геопозиціонування;

– системи вносять перешкоди в роботу бортової електроніки, включаючи системи знищення бортової електроніки (системи на базі ЕМІ, мікрохвильові системи);

– комбіновані системи РЕБ, що включають різний набір перерахованих вище опцій.

У 2015 році NEC створює систему виявлення і стеження за дронами.

У 2016 році в США, розроблено технологію, яка може ідентифікувати частоту керуючого каналу безпілотника і ставити перешкоду на цій частоті. Також система дозволяє спробувати перехопити управління безпілотником, якщо вдається ідентифікувати систему управління.

2016 Використано модель РЕБ з глушилки і з системою „злому" керуючого каналу за рахунок підбору протоколу системи управління.

Сітки. Вистрілює в сторону БЛА або швидко піднімають по курсу прямування БЛА сітки. Сітки також можуть переноситися так званими протидронами.

Традиційні. Використання дробовиків може бути при деякій удачі ефективним проти хобі-дронів. Перевірено вже в декількох інцидентах. Зокрема, в США зафіксовано близько дюжини випадків стрілянини по безпілотникам з вогнепальної зброї.

Хакінг БЛА (перехоплення управління безпілотником) Виділяють такі основні способи злому безпілотників:

1. Отримання доступу до управління за рахунок злому шифрованого каналу зв'язку або підміни даних авторизації;

2. Використання вразливостей ПЗ, включаючи переповнення буфера;

3. Використання інтерфейсів і каналів даних вихідне програмне забезпечення для „протягування" стороннього коду.

У листопаді 2015 року в США провели випробування квадрокоптера і безпілотного гелікоптера, що працюють під управлінням спеціального ПО, з підвищеною стійкістю до злому.

У Збройних Силах України, офіційно застосовуються тільки два методи: РЕБ та традиційний.

Одним із засобів є виріб „НОТА", проблемою застосування якого є відсутність досвідченого персоналу, що призначається операторами, і одночасно з цим відсутність програмного забезпечення, яке могло б допомогти працювати з даним виробом недосвідченому персоналу.

Для вирішення проблемних питань із застосування виробу „НОТА" пропонується метод триангуляції (метод визначення положення геодезичних пунктів з побудовою на місцевості систем суміжно розташованих трикутників, в яких вимірюють довжину одного боку (по базису) і кути)) та автоматичне виявлення, ідентифікація і стеження. До системи пропонується залучити не менше трьох пеленгаторів виробу „НОТА", встановлених по периметру об'єкту, що охороняється.

Усім БпЛА властива мала помітність і дуже обмежені сигнатури в більшості сфер: оптичної, акустичної, радіолокаційної та інфрачервоної.

Визначення цих сигнатур може бути реалізовано за рахунок електронного спостереження за частотами, що використовуються для контролю БпЛА або для передачі інформації інформаційною системою.

Висновок. У Збройних Силах України розробка спеціалізованого програмного забезпечення дозволить аналізувати та відстежувати навіть переповнений електромагнітний спектр, який найчастіше зустрічається в містах та серйозно ускладнює процес розпізнавання, та запропонує варіанти заходів протидії, що можуть включати як функціональне ураження (подавлення каналу управління, подавлення каналу передачі даних, подавлення каналу телеметрії, подавлення сигналу GPS-навігації), так і пряме ураження (перехоплення вогнем з гармати, стрілецької зброї або ракетою).

д.т.н. Шинкарук О. М. (НАДПСУ)
д.т.н. Лисий М. І. (НАДПСУ)
д.т.н. Бабій Ю. О. (НАДПСУ)

РОЗПІЗНАВАННЯ РУХОМОГО ОБ'ЄКТУ ТА ОЦІНКА ПАРАМЕТРІВ СИГНАЛУ ВІД СЕЙСМІЧНОГО ЗАСОБУ ОХОРОНИ КОРДОНУ

Відомо широкий клас інформаційних систем, функціонування яких включає в себе виявлення стохастичного сигналу на фоні випадкової завади, які можуть виникати в пристроях, що реєструють інформаційні сигнали (наприклад, внутрішній шум приймача), а також сигнали, які викликані діями зовнішніх джерел. Прикладами таких систем являються, окрім радіолокації, систем передачі сигналів, також сейсмічні засоби.

В даний час для охорони кордону використовуються різні технічні засоби. Серед них особливе місце займають сейсмічні засоби охорони кордону, які мають ряд переваг та забезпечують конкурентоспроможність серед інших технічних засобів. Пасивність принципу функціонування сейсмічних засобів охорони кордону і розташування сейсмоприймачів у ґрунті гарантує високий ступінь маскування. У сейсмічних засобах охорони кордону практично не існує обмежень на тип ґрунту, за винятком деяких сигналів (хиткі піски, болотисті ґрунти тощо). Висока інформативність сейсмічних сигналів дозволяє вирішувати широкий перелік завдань виявлення і розпізнавання рухомих об'єктів на великих площах, при цьому, визначаючи їх затребуваність при охороні найрізноманітніших об'єктів від периметрів приватних територій до державного кордону.

Новим класом технічних засобів охорони кордону, що набуваються інтенсивного розвитку у Державній прикордонній службі України та проходили дослідну експлуатацію у 2015-2018рр., є „Арктіум" та „Периметр-3" – це засоби охорони локальних ділянок кордону на основі трикоординатних сейсмоприймачів. Створення сучасних сейсмічних засобів охорони кордону базується на розвитку математичних методів і алгоритмів для вирішення ряду завдань, що стоять перед такими системами, вдосконаленні програмного забезпечення, а також використанні сучасних засобів обчислювальної техніки.

У доступних публікаціях з даної тематики автори, як правило, обмежуються обговоренням завдань пеленгації або визначення локального місця розташування рухомого об'єкта, не вивчаючи питання траєкторного аналізу. У таких роботах відсутній статистичний підхід до оцінки ефективності запропонованих рішень, не завжди до уваги приймаються практичні вимоги до швидкодії алгоритмів обробки інформації і до витрачених ними обчислювальних ресурсів, а також різноманітності умов, в яких реєструються реальні сейсмічні сигнали (наприклад, широкий діапазон можливих значень відношення сигнал/шум).

Серед завдань, що вирішуються з допомогою сейсмічних систем охорони кордону, можна виділити визначення місцерозташування правопорушника і аналіз його траєкторії. При схожості даної задачі з завданнями радіолокації і радіонавігації за особливістю середовища поширення сейсмічних сигналів (неоднорідність ґрунту, широкий розкид швидкостей поширення хвиль, нестаціонарність сигналів), вищенаведене призводить до низької ефективності радіолокаційних методів визначення координат і необхідності створення спеціалізованих алгоритмів для вирішення наявної проблеми. Крім того, дана задача, по-перше, може бути вирішена при використанні не усіх різновидів сейсмічних засобів охорони, по-друге, цьому питанню розробниками приділяється набагато менше уваги в порівнянні з питаннями виявлення і класифікації сейсмоактивних об'єктів. Внаслідок цього, при аналізі робіт відсутні методи вирішення зазначеного завдання, які, будучи застосовані на практиці, відповідали б усім вимогам по ефективності, темпам оновлення результатів і витраченим обчислювальним ресурсам.

Разом з тим, завдання оцінки траєкторії є досить значущою, так як при контролі обстановки на периметрах державного кордону значної протяжності (наприклад, на лініях

інженерних прикордонних споруджень) інформація, що дозволяє локалізувати місце вторгнення рухомого об’єкту і визначити напрямок та швидкість руху правопорушника, безсумнівно буде корисною для оперативної організації реагування сил охорони і своєчасного припинення можливих несанкціонованих дій.

Сейсмічні сигнали мають високу інформативність, їх аналіз дозволяє вирішувати завдання виявлення, розпізнавання і визначення координат рухомих об’єктів. При цьому, розробники сейсмічних засобів охорони стикаються з істотною нестаціонарністю і неоднорідністю характеристик сигналів, які пов'язані з наявністю різноманітних чинників (як природного, так і техногенного характеру), що заважають, а також з високою часовою та просторовою мінливістю властивостей середовища поширення сейсмічних хвиль. Процес декореляції сигналів, в якості попередньої обробки, виконується в адаптивному режимі, який супроводжує отримання поточних оцінок параметрів математичної моделі сигналу. З цих же причин всі процедури обробки, які вирішують вищеперераховані завдання, повинні адаптуватися до конкретних умов функціонування сейсмічних засобів охорони.

Один із підходів до вирішення параметричного адаптивного налаштування сейсмічних засобів охорони кордону полягає у використанні бібліотеки еталонних записів сигналів, отриманих при роботі системи в різних умовах. Безліч умов, при цьому, розбивається на групи, для кожної з яких здійснюється визначення оптимальних параметрів обробки в сейсмічних засобах охорони кордону. За участю кваліфікованих фахівців здійснюється еталонне налаштування сейсмоприймача. При налаштуванні сейсмічних засобів охорони кордону на новому об'єкті виконується оцінювання параметрів середовища, за допомогою якого умови функціонування для кожного сейсмоприймача відносяться до однієї з типових груп, представлених в бібліотеці еталонів, а параметри обробки сигналів для цього сейсмоприймача встановлюються відповідно до еталонного налаштуванням для відповідної групи.

Вирішення цього завдання вимагає розвитку методів оцінки параметрів, які можуть бути використані в якості ознак еталонних груп, з яких складена бібліотека еталонних сигналів. В якості таких параметрів обрані тимчасові параметри сейсмічного сигналу, оскільки, вони в значній мірі залежать від властивостей сейсмічного середовища. Такими параметрами є тривалість імпульсу і тривалість сукупності (пакету) імпульсів, що описують рух людини, який проходить повз сейсмоприймач. Разом із тим, поряд із завданнями адаптивного налаштування та оцінки часових параметрів сейсмічних сигналів, можливо вирішення завдання, пов’язане з визначенням поточних координат рухомого об’єкту і параметрів його руху.

Отже, мета даної роботи полягає у розвитку методів оцінки часових параметрів сейсмічних сигналів стосовно завдань обробки інформації в сейсмічних засобах охорони кордону та їх адаптивне налаштування в нестаціонарних і неоднорідних умовах функціонування.

Зміст наукових результатів полягає в тому, що вирішено завдання отримання оцінок часових параметрів сейсмічних сигналів сейсмічної системи охорони кордону, яка є важливою щодо побудови математичного та програмного забезпечення даних засобів, здійснено оцінку тимчасових даних сейсмічних сигналів сейсмоприймача, а саме: час приходу на сейсмоприймач сейсмічного сигналу, відповідно до кроків рухомого об’єкту; час приходу сигналу, відповідно надходженню рухомого об’єкту до сеймпроймача; довжину імпульсу; довжину пачки імпульсів, відповідно до відстані проходження рухомого об’єкту виявлену сейсмічним приймачем. Також здійснено дослідження алгоритмів оцінки тимчасових параметрів сейсмічних сигналів сейсмоприймача.

к.т.н. Шишацький А.В. (ЦНДІ ОВТ ЗС України)
д.т.н. Сова О.Я. (ВІТІ)

ВИКОРИСТАННЯ ЕВОЛЮЦІОНУЮЧИХ НЕЙРО-ФАЗЗІ СИСТЕМ В ЗАДАЧАХ ІНТЕЛЕКТУАЛЬНОГО ОЦІНЮВАННЯ РАДІОЕЛЕКТРОННОЇ ОБСТАНОВКИ

Актуальність проведення дослідження

Застосування сил та засобів радіоелектронної боротьби істотно впливає на ефективність ведення сучасних бойових дій, що зумовлено важливістю ролі радіоелектронних засобів в управлінні військами і зброєю.

Разом з тим, однією з характерних особливостей воєнних операцій у наш час є висока динаміка ведення бойових дій, що може бути причиною суттєвої невизначеності відносно способу застосування засобів радіоелектронної боротьби (РЕБ), при їх впливі на систему військового радіозв'язку, що є об'єктами першочергового радіоподавлення (РП).

Така невизначеність у багатьох випадках не дозволяє здійснювати оцінювання ефективності РП відомими методами та підходами, що може призводити до помилок у плануванні використання радіочастотного ресурсу засобами радіозв'язку.

Незважаючи на ефективність оцінювання радіоелектронної обстановки системами ANFIS (*Adaptive Network-Based Fuzzy Inference System* – адаптивна мережа на основі системи нечіткого виводу), відомо, що такі системи навчаються, як правило, тільки на рівні синаптичних ваг і параметрів функцій належності, причому кількість цих параметрів, а також архітектура самої нейро-фаззі системи в процесі навчання не змінюються. В той же час апріорі неможливо вибрати оптимальну структуру такої системи під час динамічної зміни радіоелектронної обстановки чи варіанту (способу) використання засобів радіоелектронної боротьби.

Тому необхідно в процесі навчання змінювати не лише такі параметри нейро-фаззі систем як синаптичні ваги і параметри функцій належності, але і архітектуру нейро-фаззі систем в цілому.

Цей напрямок досліджень є предметом так званих еволюційних нейро-фаззі систем. Але основною відмінністю більшості відомих на даний момент систем такого типу є те, що вся навчальна вибірка задана апріорі, а саме навчання відбувається в пакетному режимі. Це в свою чергу робить її малоефективною при використанні засобами радіоелектронної боротьби інтелектуальних методів подавлення та призводить до накопичення кількості помилок оцінювання.

Таким чином, на сьогоднішній день актуальною є задача розробки таких еволюційних нейро-фаззі систем, які в процесі зміни радіоелектронної обстановки в режимі реального часу змінюють як свої синаптичні ваги і параметри функцій належності, так і їх кількість та саму архітектуру системи.

Такі системи дозволяють обробляти дані, що надходять з об'єктів, що є нелінійними, нестаціонарними і можуть бути викривлені завадами апріорі невідомої природи. Варто відзначити, що актуальними є завдання розробки як систем, які навчаються з учителем, так і систем, які навчаються без учителя.

Метою зазначеного дослідження є розробка еволюційних нейро-фаззі систем і методів їх навчання, які дозволяють в режимі реального часу налаштовувати не тільки синаптичні ваги і параметри функцій належності, але і архітектуру системи в цілому.

Основні положення

В ході дослідження отримані наступні наукові результати:

1. Вперше запропоновано метод гібридного навчання еволюційної багатошарової нейро-фаззі системи, що поєднує в собі процеси еволюції архітектури, самонавчання функцій належності і контрольованого навчання синаптичних ваг, що дозволяє обробляти дані, що надходять послідовно в режимі реального часу.

2. Вперше запропоновано метод навчання еволюційних систем на основі методу групового врахування аргументів та каскадних систем обчислювального інтелекту з використанням в якості вузлів нейро-фаззі систем Ванга-Менделя, з двома входами з налаштуванням всіх параметрів функцій належності та нейро-фаззі вузлів, з двома входами що дозволяє обробляти дані в умовах коротких навчальних вибірок.

3. Вперше запропоновано метод адаптивного прогнозування нестаціонарних нелінійних часових рядів на основі еволюційної зваженої нейро-фаззі адитивної нелінійної авторегресивної моделі з екзогенними входами, що дозволяє налаштовувати як синаптичні ваги, так і архітектуру. Метод призначений для обробки даних, що надходять в режимі реального часу.

4. Удосконалено еволюційну нейро-фаззі мережу Кохонена, що кластеризується, і метод її налаштування. Суть удосконалення полягає в тому, що завдання нечіткої кластеризації потоку даних вирішується в режимі реального часу в умовах апріорної невизначеності щодо кількості кластерів.

Основними перевагами комплексу запропонованих архітектур і методів навчання є:

– однозначність отриманої оцінки радіоелектронної обстановки;

– широка сфера використання (системи радіозв'язку, радіолокації та радіоелектронної боротьби);

– простота математичних розрахунків;

– можливість адаптації до сигнальної обстановки в режимі реального часу;

– можливість синтезу оптимальної структури засобів радіомоніторингу.

До недоліків запропонованого комплексу архітектур і методів навчання слід віднести:

– втрату інформативності при оцінюванні стану радіоелектронної обстановки за рахунок побудови функції належності. Зазначена втрата інформативності може бути зменшена за рахунок вибору типу функції належності при практичних реалізаціях в засобах радіомоніторингу. Вибір типу функції належності залежить від обчислювальних ресурсів конкретного засобу радіомоніторингу;

– меншу точність оцінювання за окремо взятим параметром оцінки стану радіоелектронної обстановки;

– низьку точність оцінювання на початковому етапі, що пов'язано з ненавченістю нейронної мережі та відсутності бази сигнальної обстановки;

Висновки

Використання комплексу запропонованих архітектур і методів навчання дозволяє підвищити ефективність застосування еволюційних нейро-фаззі систем для вирішення задач прогнозування та ідентифікації даних різної фізичної природи і кластеризації в режимі реального часу.

Застосування запропонованих архітектур і методів навчання для розв'язання задач інтелектуального оцінювання радіоелектронної обстановки забезпечить:

– можливість проводити якісну обробку великих масивів різнотипних даних, що мають якісну та кількісну природу;

– скорочення обчислювальної складності за рахунок навчання нейро-фаззі системи в режимі реального часу;

– можливість зміни не тільки синаптичних ваг і параметрів функцій належності, а й архітектури нейро-фаззі системи в цілому в процесі навчання.

Запропоновані в роботі методи навчання еволюційних нейро-фаззі систем забезпечують оптимальну точність вихідного сигналу в умовах апріорної і потокової невизначеності в режимі послідовної або пакетної обробки.

Практична реалізація комплексу запропонованих архітектур і методів навчання потребує адаптації сигнального процесора конкретного засобу радіозв'язку за рахунок використання додаткового програмного забезпечення. Зокрема, можливість до розробки зазначеного програмного забезпечення надає платформа SCA 2.2 (*Software Communications Architecture*).

к.т.н. Шишацький А.В. (ЦНДІ ОВТ ЗС України)
Остапчук В.М. (в/ч А0106)
Олексенко В.П. (ВІТІ)

МЕТОДИ ОЦІНКИ СТАНУ КАНАЛУ ЗВ'ЯЗКУ НА ОСНОВІ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ, ЩО ЕВОЛЮЦІОНУЮТЬ

Актуальність проведення дослідження

Розвиток засобів радіоелектронної боротьби (РЕБ), недосконаліть відомих методів (методик) оцінки стану каналів військових систем радіозв'язку (ВСРЗ) обумовлює пошук нових наукових підходів для підвищення завадозахищеності стану каналів ВСРЗ до необхідного рівня. Зокрема, скорочення часу адаптації засобів радіозв'язку (ЗРЗ) в умовах впливу засобів РЕБ можна досягти шляхом скорочення часу, який витрачається на оцінювання стану каналу зв'язку, при збереженні необхідної достовірності. Тобто, завдання розробки нових методів оцінки стану каналу зв'язку для використання в системах та засобах РЕБ є актуальним на сьогодні.

Постановка задачі дослідження

Як відомо, класичні методи оцінки стану каналу зв'язку засновані на отриманні оцінки стану каналу зв'язку ВСРЗ за окремо взятим показником оцінки стану каналу зв'язку. Проте, враховуючи велику кількість параметрів, що впливають на стан каналів зв'язку ВСРЗ, для підвищення точності оцінювання їх стану, доцільно збільшити кількість параметрів оцінки стану каналу при збереженні прийнятної обчислювальної складності. За останні роки було представлено низку методів (методик), що застосовуються для вирішення цих завдань, серед яких одними з ефективних є штучні нейронні мережі (ШНМ). Використання персептрона, радіально-базисних мереж, автоенкодера, неокогнітрона, імовірнісних мереж виявилося досить ефективним при вирішенні широкого кола завдань.

З урахуванням вищенаведеного, метою даного дослідження є розробка методів оцінки стану каналу зв'язку на основі штучних нейронних мереж.

Основні положення

В ході дослідження отримав подальший розвиток нейромережевий метод оцінки стану каналу зв'язку на основі згорткових нейронних мереж, який передбачає використання різних функцій активації в різних шарах нейронної мережі і робастного навчання параметрів мережі, що дозволяє підвищити точність оцінки стану каналу. Суть методу полягає в тому, що на вхід нейронної мережі подаються параметри каналу (ймовірність бітової помилки, частотна характеристика каналу, імпульсна характеристика каналу та спектральна щільність потужності завади. На виході нейронної мережі, що еволюціонує, отримується узагальнена оцінка придатності стану каналу зв'язку та параметри комплексу РЕБ. На підставі отриманої інформації формується база знань радіоелектронної обстановки;

Окрім того, вперше було запропоновано метод контролю зміни стану каналу зв'язку за допомогою шаблона (типові моделі каналу), який характеризується використанням властивостей перетворення подібності стану каналу зв'язку, що дозволяє підвищити точність вимірювань. Також, удосконалено нейромережевий метод розпізнавання зміни параметрів стану каналу зв'язку, який відрізняється використанням мереж PNN (*Probabilistic Neural Networks* – ймовірнісні нейронні мережі) і CNN (*Convolutional Neural Networks* – згорткові нейронні мережі), що дозволяє підвищити точність контролю зміни стану каналів ВСРЗ і ефективність їх класифікації.

Висновки

Запропоновані методи оцінки стану каналу зв'язку на основі штучних нейронних мереж можуть бути реалізовані в засобах радіозв'язку з програмованою архітектурою. Для цього необхідно адаптувати сигнальний процесор з використанням додаткового програмного забезпечення під конкретний засіб радіозв'язку.

Шнукало А.Д. (ВІТІ)
к.т.н. Любарський С.В. (ВІТІ)

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАВДАНЬ З ПЛАНУВАННЯ ОРГАНІЗАЦІЇ ЗВ'ЯЗКУ В АВТОМАТИЗОВАНІЙ СИСТЕМІ УПРАВЛІННЯ ЗВ'ЗКОМ

Актуальність дослідження обумовлена необхідністю вдосконалення системи управління зв'язком Збройних сил України і, як слідство, у підвищенні ефективності задачі планування організації зв'язку.

Витрати часу та складність реалізації планування збільшується при переході від нижчого рівня до верхнього, а конкретизація кожної задачі планування, навпаки, зменшується. Звідси випливає, що порівневе узгодження рішення задач автоматизації планування є важливим питанням, що визначає ефективність функціонування системи управління зв'язком в цілому.

Мета дослідження полягає у підвищення ефективності процесів планування бойового застосування частин, підрозділів зв'язку за рахунок виконання **наступних часткових завдань дослідження**:

– аналіз сучасного підходу у плануванні системи зв'язку у Збройних силах України, спираючись на вимоги керівних документів з організації зв'язку;

– вдосконалення самого алгоритму планування організації зв'язку та процесів, що пов'язані з цією задачею, з урахуванням недоліків та обмежень сучасної моделі;

– автоматизація процесів планування організації зв'язку за рахунок розробки програмного модулю планування завдань з організації зв'язку автоматизованої системи управління зв'язком (АСУЗ). Апробація моделей.

Виклад основного матеріалу. Автоматизація процесів планування є важливою функцією управління, яка представляє собою процес постановки завдань (вироблення рішень) за менш короткий проміжок часу, розробки програм їх досягнення, що оформлені у вигляді сукупності документів. Змістом процесу планування є розподіл ресурсів системи, підрозділів автоматизації, визначення порядку їх використання для досягнення поставлених цілей. Одне з основних завдань при створенні складної автоматизованої системи управління організаційного типу є проектування її структури, яка визначає внутрішню організацію і відносно стійкі взаємозв'язки елементів системи. Рішення даного завдання являє собою складний трудомісткий процес, так як на ранніх стадіях проектування параметри системи в ряді випадків можуть бути відомі лише приблизно, з деяким розподілом ймовірностей їх значень або з деяким ступенем приналежності значень параметрів заданими інтервалами, що призводить до неоднозначності визначення структури системи. Облік динаміки функціонування системи на етапі її проектування призводить до необхідності спільного використання оптимізаційних та імітаційних моделей для отримання оптимальних (раціональних) варіантів побудови системи. В даній роботі для вирішення завдання проектування структури автоматизованої системи управління зв'язком (АСУЗ) запропоновано використання агрегативно-декомпозиційного підходу.

Базуючись на етапи проектування структури системи, використовуючи класичний підхід проектування було розроблено узагальнену архітектуру і алгоритми роботи програмного модулю планування завдань з організації зв'язку.

Під час оцінки ефективності отримано приблизний результат затрат часу на прийняття управлінських рішень. Коефіцієнт відносної економії часу у випадку частоти рішення задач 5 разів за добу дорівнює приблизно 12 %.

Висновки. Отже, в роботі запропоновано використання агрегативно-декомпозиційного підходу для проектування структури АСУЗ та на його основі реалізовано програмний модуль планування завдань з організації зв'язку. Програмний модуль був апробований в ході роздільного штабного тренування, що відбувалось в ГУЗіС ГШ ЗСУ.

Шолудько В.Г. (ВІТІ)
Андріюк М.С. (ВІТІ)

ОРГАНІЗАЦІЯ СУПУТНИКОВОГО ЗВ'ЯЗКУ В МЕХАНІЗОВАНОМУ БАТАЛЬЙОНІ. ПЕРСПЕКТИВИ УДОСКОНАЛЕННЯ ЗАСОБІВ СУПУТНИКОВОГО ЗВ'ЯЗКУ

Для організації супутникового зв'язку в мб використовується ССЗ „TOOWAY". Використовується супутник на геостаціонарній орбіті, який покриває зону Західної і Східної Європи. Організаційно і технічно мережа супутникового зв'язку представляє собою об'єднання радіоліній супутникового зв'язку, розгорнутих у відповідності зі структурою управління.

При роботі в мережі підлеглі станції знаходяться в режимі чергового прийому і включаються на передачу з дозволу головної станції чи за розкладом. В напрямках і мережах супутникового зв'язку станція старшого командира (штабу) являється головною. В напрямках і мережах взаємодії головна станція призначається штабом, який організує взаємодію. На теперішній час на озброєнні військ знаходяться станції супутникового зв'язку „Tooway" з телекомунікаційним обладнанням.

Для організації супутникового зв'язку в мб є КШМ БМП-1КШ (Р-145БМ) з станцією супутникового зв'язку „Tooway" та телекомунікаційним обладнанням до складу якого входить:

– блок прийомо-передавача з антеною;
– модем;
– маршрутизатор (на 4 порти і більше);
– два VoIP-шлюзи, телефонні апарати, ноутбуки.

Для закриття каналів зв'язку або групових цифрових потоків використовується АПК „Г". Якщо він стоїть перед маршрутизатором то закривається увесь цифровий потік. Станція супутникового зв'язку з телекомунікаційним обладнанням забезпечує напрямок супутникового зв'язку між КСП мб і КП мбр. В залежності від цифрового потоку (ресурсу супутникового зв'язку) можливе отримання різної кількості каналів.

При швидкості 512 кб/с можливо отримати 1 – 2 відкритих телефонних каналів, 1-2 закритих телефонних каналів, автоматизоване робоче місце ЛОМ АСУ ПД „Дніпро" і 1 IP – канал для ретранслятора DR-3000. З метою розширення зони покриття, або забезпечення зв'язку між територіально-розосередженими абонентами (в межах мбр (БрТГ)) створюється декілька сайтів.

Ретранслятори сайтів однієї системи з'єднуються між собою IP-каналами. Така конфігурація називається „IP-siteconnect". Всього у системі може бути до 15 сайтів. Ретранслятор одного із сайтів призначається головним („Master") на КП БрТГ, а інші підлеглі („Slave"). При об'єднанні ретрансляторів є можливість створити між ними захищені канали VPN (Virtual PrivateNetwork).

Якщо абонент, який знаходиться у зоні одного ретранслятора, посилає виклик абонентам (абонентів) у зоні дії іншого, усі ретранслятори отримають цей виклик абонента на встановлення з'єднання, посилають запит, щоб визначити де знаходиться потрібний абонент і ретранслює сигнал тільки той ретранслятор, на каналі якого знаходиться абонент, якого викликають.

З метою створення конфігурації IP-Site-Connect для об'єднання ретрансляторів використовуються IP-канали, створені ССЗ мб (можливо рр/ст.) Таким чином при організації супутникового зв'язку на напрямку зв'язку КСП мб – КП мбр можливо розгорнути) – організація ЛОМ АСУ ПД „Дніпро"; - організація IP-Site-Connect – для організації мережі ретрансляторів; - 1-2 ТФ канал супутникового зв'язку для організації зв'язку з КП мбр; - 1-2 ТФ канали супутникового зв'язку для організації зв'язку з КП сектора АТО.

Способи організації супутникового зв'язку в механізованому батальйоні.

Напрямок супутникового зв'язку – спосіб організації супутникового зв'язку між двома командирами (штабами), при якому зв'язок здійснюється по окремій лінії супутникового зв'язку, розгорнутій безпосередньо між ними. (рис.1)

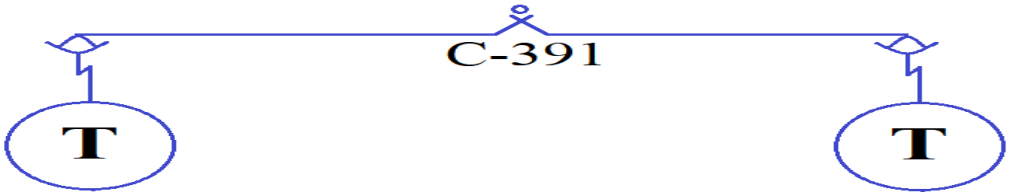


Рис.1. Напрямок супутникового зв'язку

Мережа супутникового зв'язку – спосіб організації супутникового зв'язку, при якому зв'язок командира (штабу) з декількома командирами (штабами) підлеглих і взаємодіючих частин. (Рис-2)

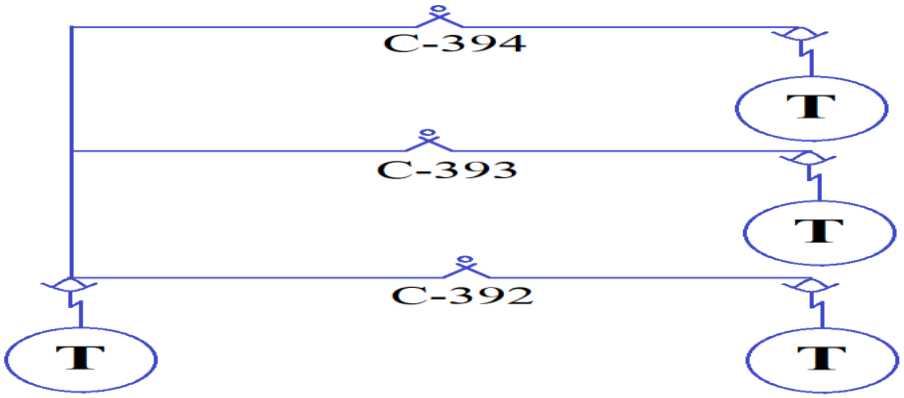


Рис.2.Мережа супутникового зв'язку

Перспективи використання та розвитку засобів супутникового зв'язку

На даний час основні зусилля провідних країн світу спрямовані на створення багатофункціональних, енергоємних космічних апаратів і мало габаритних земних станцій, підвищення завадостійкості напрямків зв'язку за рахунок використання нових типів сигналів, застосування багатопроменевих адаптивних антенних систем і компенсаторів перешкод, реалізація високошвидкісних режимів передачі інформації.

На цей час у ЗСУ розгорнута повнозв'язна підсистема супутникового зв'язку, яка доведена до окремих батальйонних та ротних тактичних груп, ротних та взводних опорних пунктів. З метою підвищення живучості системи супутникового зв'язку розглядається рішення щодо нарощування системи засобами Ku-діапазону.

Для забезпечення потреб ЗС України у сучасних засобах радіозв'язку пропонується налагодити виробництво іноземних засобів радіозв'язку військового призначення на території України.

Також пропонується розпочати роботи щодо відновлення державної програми із запуску національного супутника зв'язку та створення вітчизняного виробництва станцій супутникового зв'язку військового призначення з можливістю організації зв'язку (обміну інформацією), як в стаціонарному виконанні так і в русі. У разі відсутності достатнього фінансування пропонується розглянути можливість закупівлі чи лізингу станцій супутникового зв'язку військового призначення у закордонного виробника.

Шпак О. О. (ВІТІ)
д.т.н. Сова О. Я. (ВІТІ)

МОДЕЛЬ АВТОМАТИЗОВАНОЇ СИСТЕМИ ЛОГУВАННЯ НА ОСНОВІ СТЕКУ ELK+KAFKA ДЛЯ ВІДСЛІДКОВУВАННЯ ТА АНАЛІЗУ ПОДІЙ У МЕРЕЖАХ

У сучасних мережах, із великою кількістю мережевого та серверного обладнання постає питання автоматизованого налаштування систем, що спростить роботу адміністратора у підтриманні належного стану та безпеки пристроїв, а також у моніторингу їх роботи.

Для моніторингу помилок, зауважень, сигналів небезпеки, аутентифікації та авторизації на мережеве та серверне обладнання, дій, вчинених з пристроями як авторизованими так і неавторизованими користувачами, необхідна система, яка буде візуалізувати ці події на основі проаналізованих та відфільтрованих даних. З цією метою використовуються лог-повідомлення, які, на етапі створення, складаються з великої кількості полів, структура і формат яких не забезпечує можливість швидкого та якісного аналізу інформації. Із зростанням кількості повідомлень у мережі, з'являється потреба у їх фільтрації, яка здійснюється з метою відсіювання інформації, що є менш важливою в рамках моніторингу. Надалі, повідомлення повинні бути збережені, для чого доцільно використати індексні розподілені сховища, які забезпечують можливість гнучкого пошуку за окремим символами.

Сьогодні, для аналізу подій в інформаційно-телекомунікаційних мережах ЗС України використовується система моніторингу стану мережі Zabbix, яка отримує інформацію за допомогою SNMP- протоколу. Він передає дані про стан мережевих пристроїв, проте, не дає можливості здійснювати обробку інформації, наприклад, швидко знайти необхідне повідомлення на основі окремих символів. Zabbix працює з метриками, які представлені в неструктурованому вигляді, через що є неінформативними, хоча надають уяву про те, які процеси відбуваються у мережі. При роботі з даними Zabbix не дає можливості архівувати інформацію за визначений період і це не дозволяє керувати об'ємами даних у сховищі.

У ході проведеного дослідження, з урахуванням вищезазначених недоліків, запропоновано систему на основі open-source стеку продуктів ELK+KAFKA, до якої входять: Syslog-ng сервер та сервіси Apache Kafka, Filebeat, Logstash, Elasticsearch, Kibana. Syslog-ng отримує повідомлення з мережевих пристроїв та серверного обладнання, працюючи за UDP та TCP протоколами. Filebeat зчитує повідомлення із syslog-ng серверу, ПК, віртуальних машин і транспортує дані до Apache Kafka – сервісу, який виступає буфером збору повідомлень, що може працювати з великими масивами даних. Kafka дозволяє сортувати дані за категоріями, наприклад, кожне повідомлення буде записуватися до різних розділів в залежності від його важливості. Це забезпечує структурування даних та готує їх для подальшої обробки. Із Kafka повідомлення зчитує Logstash, який виступає у ролі фільтру для повідомлень та сервісу, що пересилає дані до сховища даних. На цьому етапі, менш важлива інформація відсіюється та при потребі зміст повідомлення розбивається на окремі слова за допомогою фільтрів. Logstash передає дані до розподіленого індексного сховища даних Elasticsearch, перевагами якого є швидкодія, відмовостійкість, розподіленість, масштабованість. Сховище надає унікальний код кожному символу у повідомленні, що дозволяє здійснювати гнучкий пошук серед великих масивів даних. Kibana як кінцевий сервіс візуалізує проаналізовані і відфільтровані дані та дозволяє будувати графіки і діаграми з різними значеннями та відповідно до часу отримання повідомлення, що дає змогу краще виявляти проблеми у мережевій інфраструктурі. У якості захисту каналів передачі інформації використовується TLS/SSL протоколи.

Таким чином запропонована система побудована на open-source продуктах, забезпечує гнучке налаштування, належний рівень безпеки, досить легка в адмініструванні, та надає зручну візуалізацію для аналізу подій у мережевій інфраструктурі.

Якорнов Є.А. (НТУУ „КПІ ”)
Цуканов О.Ф. (НТУУ „КПІ ”)

АЛГОРРИТМ ОЦІНКИ ПАРАМЕТРІВ РУХУ БЕЗПІЛОТНИХ ЛЕТАЛЬНИХ АПАРАТІВ

Розглядається алгоритм оцінювання параметрів руху безпілотних літальних апаратів як елементів літаючих бездротових сенсорних мереж FANET. Для оцінки параметрів руху запропонований стійкий алгоритм динамічної фільтрації дозволяє отримати оцінки координат і їх похідних. Отримані результати роботи дозволяють одночасно підвищити точність оцінювання параметрів руху, забезпечити стійкість процесу оцінювання та ефективність управління елементами бездротової сенсорної мережі FANET.

В даний час, відбувається інтенсивне використання можливостей одиночних і безпілотних літальних апаратів (БПЛА) в складі групи в різних сферах діяльності людей, в тому числі, і в мобільних літаючих сенсорних мережах FANET [1].

Для ефективного управління угрупованням з М БПЛА на наземному пункті недостатньо знати тільки їх поточні координати в реальному масштабі часу, одержуваних, наприклад, за допомогою бортових датчиків GPS. Для вирішення завдання управління необхідна інформація про швидкостях і прискореннях, ці параметри залежать від багатьох факторів і, насамперед, від технічного стану самого літального апарату і стану атмосфери на траєкторії його польоту. Крім того, в разі втрати управління з наземного пункту повинно бути передбачено автономне управління з одного з БПЛА мережі. Координати БПЛА можуть бути визначені як за допомогою датчиків GPS встановлених на всіх БПЛА так і шляхом взаємного вимірювання відстаней D_{ij} між і-тим і j-тим БПЛА наприклад, з використанням протоколів IEEE 802.15.4 ZigBee, 6LoWPAN, Thread, RPL [2], в такому випадку датчиками GPS оснащуються тільки 3-4 БПЛА мережі. Метою роботи є розробка високоточного і одночасно стійкого алгоритму оцінювання ВС (параметрів руху) елементів FANET на базі БПЛА на основі інформації про координатах і їхніх помилках в даний момент часу.

Метою роботи є розробка високоточного і одночасно стійкого алгоритму оцінювання ВС (параметрів руху) елементів FANET на базі БПЛА на основі інформації про координатах і їхніх помилках в даний момент часу.

Математична постановка задачі оцінювання ВС БПЛА як елементів FANET при їх квазіоднородном розподілі в просторі виглядає наступним чином.

На підставі наявної інформації про координати $\widetilde{x_i}$, $\widetilde{y_i}$, $\widetilde{z_i}$, і їх середньоквадратичних помилки (СКП) $\widetilde{\sigma x_i}$, $\widetilde{\sigma y_i}$, $\widetilde{\sigma z_i}$, необхідно визначити параметри руху - оцінки ВС $\overrightarrow{X_n}$ координати $\hat{x_i}$ $\hat{y_i}, \hat{z_i}$, , похідних (швидкостей) $\hat{\dot{x}_i}, \hat{\dot{y}_i}, \hat{\dot{z}_i}$ і коваріационную матрицю (КМО) помилок оцінки координат елементів K_n і надалі після чергового етапу вимірів відстаней між сусідніми БПЛА виробляти їх уточнення.

СКО визначення координат БПЛА $\widetilde{\sigma x_i}$, $\widetilde{\sigma y_i}$, $\widetilde{\sigma z_i}$, отриманих шляхом вимірювання взаємних відстаней між БПЛА мережі визначаються багатьма факторами і залежать від динаміки (швидкості і прискорення польоту БПЛА) сезонної, тимчасової нестабільності гравітаційного поля Землі, від умов поширення радіохвиль і т.д.

СКО визначення координат БПЛА $\widetilde{\sigma x_i}$, $\widetilde{\sigma y_i}$, $\widetilde{\sigma z_i}$, отриманих шляхом вимірювання взаємних відстаней між БПЛА мережі визначаються багатьма факторами і залежать від динаміки (швидкості і прискорення польоту БПЛА) сезонної, тимчасової нестабільності гравітаційного поля Землі, від умов поширення радіохвиль і т.д.

Для отримання високоточних оцінок параметрів руху при багаторазових вимірах пропонується використовувати алгоритм оцінювання на основі фільтра Калмана [3].

Вектор стану: $X_{in}{}^{T} = |x_{in},\ \dot{x}_{in},\ y_{in},\ \dot{y}_{in}, z_{in}, \dot{z}_{in}|,$

вектор вимірів: $Y_{in}{}^{T} = |\widetilde{x_{in}}\ ,\ \widetilde{y_{in}},\ \widetilde{z_{in}}|$

величини якого визначаються шляхом вимірювання відстаней між БПЛА.

Екстрапольоване значення ВС X_{in}^{e}

$$X_{\text{in}}^{e} = F_{in,n-1}X_{in-1} + G_{n-1}U_{n-1}, \quad (1)$$

де $F_{in,n-1}$ – матриця екстраполяції, G_{n-1} - матриця управління, $U_{\text{n}-1}$ – вектор управління; S_{n-1} – КМО вектора управління, S_{n-1}^{*} уточнене значення апріорної КМО вектора управління, X_{in}^{e} вктроп стану на n-1 кроці.

$$S_{n-1}^{*} = S_{n-1}\gamma, \quad (2)$$

де γ – параметр стійкості процесу оцінювання, екстрапольована апріорна КМО

$$K_{in}^{e} = F_{in,n-1}\,K_{in-1}F_{in,n-1}{}^{\text{T}} + \text{G}_{\text{n}-1}S_{n-1}^{*}G_{\text{n}-1}^{T}, \quad (3)$$

де K_{in-1}– апріорная КМО, Q_{in} - КМО вектору вимірювань Y_{in}, на n - му кроці.

Коефіцієнт посилення

$$H_{in} = K_{in}^{e}(K_{in}^{e} + \text{Q}_{in})^{-1}, \quad (4)$$

Оцінка ВС, $$\widehat{X_{in}} = X_{in} + H_{in}(Y_{in} - X_{in}^{e}), \quad (5)$$

Апостеріорна КМО оцінювання

$$\widehat{K_{in}} = K_{in}^{e} - K_{in}^{e}\ H_{in}. \quad (6)$$

Крім того, розглянутий алгоритм оцінювання (1) – (6) дозволяє забезпечити стійке оцінювання ВС в тому числі, і при раптовій зміні траєкторії руху БПЛА.

Дослідження даного алгоритму здійснювалося методом математичного моделювання.Отримані характеристики за результатами моделювання польоту БПЛА при прямолінійній русі БПЛА і наступних видів маневру: відхід від лобового зіткнення, набір висоти і плавний розвороту на 90^{0} с з наступним переходом до прямолінійного руху.

При γ = 0, алгоритм має місце розбіжність процесу оцінювання, іншими словами, відомий фільтр Калмана не стійкий.

Для 0.4 ≤γ≤0.8 запропонований алгоритм дозволяє отримати стійке оцінювання параметрів руху БПЛА.

При прямолінійному русі максимальна помилка за координатами становить 4,5 м. – γ = 0.1, а мінімальна 1.6 м. – γ = 0.8.

На ділянці маневру: максимальна помилка за координатами 18 м., – γ = 0.1, а мінімальна 5 м. – γ = 0.4, максимальна помилка за швидкостями становить 18 м / с., – γ = 0.1, а мінімальна 10 м / с. – γ = 0.8.

При цьому оптимальне значення γ за допомогою якого отримані мінімальні помилки і забезпечується стійкість процесу оцінювання параметрів руху БПЛА як елементів FANET становить 0.8. Мінімальне значення помилок за координатами і швидкостями на ділянці маневру, досягається в середньому за 8 кроків оцінювання.

Результати моделювання з використанням імітаційного моделювання дозволяють стверджувати, що запропонований стійкий алгоритм оцінювання при багаторазових вимірах відстаней між БПЛА дозволяє отримати стійкі оцінки ВС координат і їх похідних і при цьому підвищити точність визначення координат БПЛА мережі FANET, в тому числі і при неточної інформації про помилки вимірювання відстаней.

ЛІТЕРАТУРА

1. Романюк В., Степаненко Є.О., Панченко І., Восколович О.І. Літаючі самоорганізуючі радіомережі. Збірник наукових праць ВІТІ № 1 – 2017, стор. 105-114.

2. Langdon M. ZigBee goes underground, E&T Magazine, 2009, Aug.

3. Grewal M.S., Andrews A.P., Kalman Filtering – Theory and Practice Using MATLAB», Wiley, 2001.

Якорнов Є.А. (НТУУ „КПІ ”)
Цуканов О.Ф. (НТУУ „КПІ ”)

АЛГОРИТМИ РОЗПОДІЛУ РІЗНОРІДНИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ДЛЯ НАНЕСЕННЯ УДАРІВ ПО ОБ'ЄКТАМ, ЯКІ ЧИНЯТЬ ОПІР

Безпілотні літальні апарати (дрони) знаходять все більше застосування в різних областях діяльності людства, і, в першу чергу, у військовій сфері [1]. Сучасні дрони можна застосовувати в якості активних засобів для знищення наземних об’єктах так і засобі радіоелектронної боротьби, для придушення наземних радіоелектронних об’єктів. Маючи угрупування які складаються з ударних дронів та дронів оснащених засобами радіоелектронного придушення (РЕП), можна ефективно вирішувати задачу знищення наземних об’єктів , які чинять опір.

Метою роботи є розробка алгоритму формування угрупування БПЛА для вирішення задач нанесення ударів за допомогою дронів з заданими вимогами.

Розглянемо 2 групи дронів, перша група ударних дронів, яка призначена для знищення наземних об’єктів, інша група для оснащених засобами РЕП.

Відомі ймовірності знищення P_1 та РЕП P_2, відомі також коефіцієнти втрат ударних дронів C_1 та дронів РЕП C_2. Необхідно знайти оптимальне значення кількісті дронів першої $X_1^{опт}$ та другої груп $X_2^{опт}$, забезпечують задану імовірність знищення ураження об’єкта $W_з$

$$W_з = 1-(1-P_1)^{x_1-\alpha_1}(1-P_2)^{x_2-\alpha_2} \quad (1)$$

де: x_1, x_2 – кількість дронів першої та другої групи,

P_1 – імовірність ураження ударним дроном, P_2 – імовірність дроном дроном РЕП,

α_1, α_2 – мінімальне можливий наряд дронів, β_1, β_2 – мінімально можливий наряд дронів.

Необхідно виконання обмежень:

$$\alpha_1 \le x_1 \le \beta_1, \quad \alpha_2 \le x_2 \le \beta_2, \quad (2)$$

та забезпечує мінімум втрат Y:

$$Y = c_1x_1 + c_2x_2. \quad (3)$$

Необхідно розподілити ударні дроні та дроні РЕП, щоб при заданій імовірності ураження P_1та придушення P_2, обмеженнях α_1, α_2 та β_1, β_2 втрати своїх дронів були б мінімальними. Тобто значення функціонала (2) мінімальне значення.

Вказана задача відноситься до задач нелінійного програмування та може бути вирішена методом прирощень [2]. Сутність метода полягає в мінімізації цільової функції (3) шляхом послідовного знаходження шуканих значень змінних $x_1^{опт}$, $x_2^{опт}$ методом послідовних наближень (ітерацій).

В якості початкових значень змінних X_0 =(x_{10}, x_{20}) беруться їх мінімальні значення α_1, α_2 як правило $\alpha_1 = 1$, α_2=1.

–на першому кроці ітерацій кожному зі значень x_{10}, x_{20} дається визначене прирощення Δx_{10} та Δx_{20} відповідно обмежень (3). Отримані за результатом змінні являють собою „чистий” набір X_1= (x_{11}, x_{21});

– з X_0, X_1 складаються два комбінованих наборі в кожному з яких один з аргументів має нове значення другій залишається без змін;

– на другому кроці за допомогою прирощень збільшуються значення аргументів x_1, x_2 комбінованих наборів виходячи із обмежень (3) та знову отримують „чисти" значення та нові комбінаційні набори і т. і.; (3)

– на кожному кроці ітерацій для „чистих" і комбінованих наборів змінних обчислюються значень цільової функції Y, мінімально значення цільової функції. Мінімальне значення цільової функції на n – ному кроці ітерацій по всім „чистих" наборам на даному і минулому кроках позначимо $\bar{Y}_n$, а по всіх комбінованих через $\overline{\bar{Y}_n}$.

– процес ітерацій продовжується до тих пір поки

$$\bar{Y}_n - \overline{\bar{Y}_n} \leq \varepsilon \qquad (4)$$

де: ε – потрібна точність рішення задачі.

Надаємо алгоритм розрахунків за методом прирощень:

1. складається початковий набір аргументів: $X_0 = (x_{10}, x_{20}), \alpha_1, \alpha_2$;
2. розраховуються прирощення Δx, які визначаються як значення зворотні до втрат:

$$\Delta x_{10} = t/c_1, \quad \Delta x_{20} = t/c_2.$$

параметр t визначає швидкість збіжності алгоритму і розраховується на підставі обчислення виразу (1) для W = 0, розрахунки показують що $1.0 \leq t \leq 1.3$.

3) виконується перший крок $x_{11} = x_{10} + \Delta x_{10}$, $x_{21} = x_{20} + \Delta x_{20}$, отримаємо чистий набір, $X_1 = (x_{11}, x_{21})$, складаємо два комбінованих набора (x_{11}, x_{20}), (x_{10}, x_{21}),

4) для одного чистого, та двох комбінованих обчислюємо значення цільової функції (1)

перевіряємо умову (1), в разі і виконання для наступного розрахунку беремо значення, X_1

5) на наступному кроці розраховуємо нове значення $X_{1н}$ та комбіновані набори

$$(x_{11н}, x_{20н}), (x_{10н}, x_{21н}),$$

6) значення цільової функції розраховуємо для двох „чистих" наборів та двох комбінованих,

7) перевіряємо умову (4) та обмеження (2) , як що вони не виконуються переходимо до наступного кроку, інакше отримане значення скругліємо x_{1n}, x_{2n} є результатом рішення задачі.

Отриманий результат є оптимальним планом розподілення різнорідних дронів для нанесення по наземних об'єктах, які чинять опір.

Запропонований алгоритм може бути застосований для рішення задачі в разі наявності більш двох груп різноманітних дронів. Крім того, р алгоритм можна застосовувати під час планування комбінованого удару і по декільком різноманітним наземним об'єктам які чинять опір.

ЛІТЕРАТУРА

1. Романюк А.В. Метод збору інформації моніторингу в бездротових сенсорних мережах з використанням безпілотних літальних апаратів. Збірник наукових праць ВІТІ. Київ, – 2018. № 1, с. 90 – 99.

2. Лисенко О.І., Тачинина О.М , Алексєєва І.В. Математичні методи моделювання та оптимізації. ч.1.Математичне програмування та дослідження операцій. Підручник. – К.: НАОУ, 2017.– 212 с.

Яровий В.С. (ВІТІ)
к.т.н. Радзівілов Г.Д. (ВІТІ)
к.т.н. Гладких В.М. (ВІТІ)

ПРОБЛЕМИ РОЗВИТКУ СИСТЕМИ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ ТА РЕМОНТУ ЗАСОБІВ ЗВ'ЯЗКУ І АВТОМАТИЗАЦІЇ ЗБРОЙНИХ СИЛ УКРАЇНИ

Актуальність, постановка задачі. Аналіз відмов новітніх засобів зв'язку і автоматизації показав, що більшість з них відбулися внаслідок неправильної експлуатації та відсутності будь-яких видів ЗІП і вимірювальної апаратури до них. Окрім того, на даний час відсутня статистика щодо виходу з ладу елементів від часу їх напрацювання на відмову. Наявна інформація щодо кількісних та якісних показників стосовно поставлених у Збройні Сили України зразків не дозволяє проводити розрахунки щодо кількості та комплектності відповідних видів ЗІП на сучасну техніку.

Згідно з ГОСТ В 15.705 – за розробку видів ЗІП, їх комплектність, кількість, якість та норми їх витрат відповідає тільки головний розробник (розробник), при чому методику розрахунку складу комплектів ЗІП розробник повинен узгоджувати з замовником.

Усі системи, комплекси, засоби зв'язку та автоматизації, крім радіорелейних станції Р-425С1, Р-425С2, Р-425С3, Р-414МУ авто., Р-414МУ-01 авто., Р-414МУ-02 авто., Р-414МУ-03 авто, виробів В271-Л, О171, О171-01, були прийняті на постачання (озброєння) в результаті проведення ініціативних ДКР, визначальних відомчих випробувань або матеріальної допомоги іноземних країн, згідно Постанови Кабінету Міністрів України від 25 лютого 2015 року № 345 (зі змінами).

Мета. Метою доповіді є визначення проблем розвитку системи технічного обслуговування та ремонту засобів зв'язку і автоматизації Збройних сил України.

Основні положення. Система технічного обслуговування та ремонту засобів зв'язку і автоматизації відіграє значну роль в підтриманні у справному або працездатному стані засобів зв'язку і автоматизації при їх зберіганні, транспортуванні, підготовці до використання за призначенням, використанні за призначенням в стаціонарних та польових умовах і є складовою частиною системи технічного забезпечення зв'язку і автоматизації.

В основу діючої системи ремонту техніки зв'язку і автоматизації ЗСУ покладена стратегія ремонту за напрацюванням, при якій перелік та періодичність виконання операцій залежать від напрацювання виробу з початку експлуатації чи після чергового ремонту. Існуюча система ремонту є планово-запобіжною і характеризується визначенням для кожного об'єкта фіксованого обсягу робіт через заплановані інтервали напрацювання.

Новітня техніка зв'язку, що надходить на постачання, не передбачає можливості проведення на ній будь-якого ремонту силами і засобами ремонту і обслуговування військ зв'язку, через відсутність технічної документації, документації з ремонту і номенклатури ЗІП для неї та апаратних технічного забезпечення з обладнанням, що забезпечить виконання відповідних робіт в польових умовах.

Діюча система технічного обслуговування та ремонту засобів зв'язку і автоматизації не відповідає в повному обсязі покладеним завданням, що стоять перед військами зв'язку ЗСУ.

Отже основними проблемами розвитку системи технічного обслуговування та ремонту засобів зв'язку і автоматизації ЗСУ є:

відсутність в державі органу з планування та контролю за розробленням і виробництвом військової техніки при Кабінеті Міністрів України;

відсутність керівних документів Міністерства оборони України та Генерального штабу ЗСУ, що регламентують ремонт та сервісне обслуговування за технічним станом;

відсутність необхідних ремонтних комплектів типу ЗІП-О, ЗІП-Г, ЗІП-Р на новітні засоби зв'язку і автоматизації, які постачаються до ЗСУ;

відсутність оперативних (стратегічних) та військових запасів на покриття потреби в ЗІП частин та підрозділів ЗСУ та тих, що формуються;

неможливість проведення певних видів поточного та середнього ремонту новітніх засобів зв'язку і автоматизації у військових частинах в стаціонарних та польових умовах внаслідок відсутності ремонтної документації на них, відповідних засобів і приладдя, засобів вимірювання для проведення необхідних видів ремонту та навченого особового складу;

необхідність розробки, виготовлення та постачання до ЗСУ сучасних (модернізації існуючих) апаратних технічного забезпечення, обладнаних засобами технічного обслуговування та ремонту, що забезпечить виконання відповідних робіт з новітніми (іноземними) засобами зв'язку і автоматизації в польових умовах;

відсутність науково обґрунтованих методик визначення параметрів засобів зв'язку і автоматизації, які б дозволяли дати достовірну оцінку ефективності метрологічного обслуговування засобів зв'язку ЗСУ;

застарілість наявних засобів вимірювальної техніки, які не враховують сучасні тенденції зарубіжного приладобудування;

відсутність гармонізації військових стандартів з державними стандартами, що застосовуються в інших сферах, але регулюють такі самі питання, з відповідними міжнародними, європейськими стандартами та стандартами країн членів НАТО щодо впровадження та проведення технічного обслуговування та ремонту на сучасних засобах зв'язку і автоматизації, які знаходяться на постачанні у ЗСУ;

відсутність механізму розроблення і виробництва військової техніки у відповідності з вимогами Закону України „Про державне оборонне замовлення";

відсутність визначеного порядку участі суб'єктів господарської діяльності приватної форми власності у супроводженні стадій життєвого циклу поставленої до ЗСУ військової техніки;

повна залежність ЗСУ від приватних та іноземних підприємств щодо проведення технічного обслуговування та ремонту на отриманих засобах зв'язку і автоматизації;

відсутність порядку забезпечення справності, технічної придатності та модернізації військової техніки іноземного походження, прийняття її на озброєння;

використання застарілої планово-запобіжної системи ремонту за напрацюванням;

відсутність рішення щодо створення сервісних центрів (підрозділів) технічного обслуговування і ремонту на базі ремонтних установ, військових частин із залученням представників виробників сучасних та перспективних засобів зв'язку;

низький рівень системи технічного забезпечення засобів зв'язку і автоматизації ЗСУ щодо організації управління системою технічного обслуговування та ремонту засобів зв'язку і автоматизації та підготовки відповідних фахівців;

відсутність системи моніторингу кількісних та якісних показників щодо відмов сучасних засобів зв'язку і автоматизації.

Висновки. Таким чином, існуюча система технічного обслуговування та ремонту засобів зв'язку і автоматизації в умовах сьогодення є застарілою і потребує вдосконалення. Тому існує нагальна потреба у розробці Концепції розвитку системи технічного обслуговування та ремонту засобів зв'язку і автоматизації у військах зв'язку Збройних Силах України, загальні положення якої відповідатимуть реаліям експлуатації новітніх засобів зв'язку і автоматизації.

Ярошенко Р.Р. (ВІТІ)
Нерознак Є.І. (ВІТІ)

РОЗПОДІЛЕНА СИСТЕМА ЦЕНТРАЛІЗОВАНОГО ЗБОРУ, ЗБЕРІГАННЯ ТА ОБРОБКИ ДАНИХ НА ОСНОВІ NEXTCLOUD

Актуальність проведення дослідження

Як свідчать світові тенденції розвитку IT-індустрії, переважна більших сучасних інформаційних систем будуються за централізованою архітектурою. Яскравим підтвердженням цього факту є вибуховий розвиток хмарних (cloud) технологій як глобального тренду.

Базовим стимулом до розвитку саме такої архітектури є стрімка еволюція телекомунікаційних сервісів, підвищення їх надійності та пропускної спроможності, зниження вартості послуг передачі даних, широке проникнення як в географічному сенсі, так і серед різних верств населення, бізнесу.

Як правило, централізована система будується з використанням сучасної трирівневої архітектури та web-технологій, на базі потужного високонадійного центру обробки даних (ЦОД).

Разом з тим централізований варіант архітектури характеризується наступними негативними властивостями:

- підвищені вимоги до потужності апаратного забезпечення центрального рівня та рівня готовності ;
- необхідність забезпечення постійного телекомунікаційного зв’язку з центром ;
- необхідність забезпечення централізованої процедури реєстрації та ведення всіх користувачів системи;

У зв'язку з цим ***метою даного дослідження*** є розробка розподіленої системи збору, зберігання та обробки даних на основі NEXTCLOUD;

Основною ознакою розподіленого варіанту архітектури інформаційної системи є наявність в кожній точці її впровадження (вузлі) повноцінного клієнт-серверного комплексу з локальною базою даних.

Основним завданням є організація ефективного доступу користувачів до інформаційних і програмних ресурсів та ефективна взаємодія як користувачів з ресурсами, так і різних видів ресурсів між собою.

Таким чином, до переваг розподілених систем можна віднести: масштабованість, наявна інтеграція рішень, поступове системне розширення, ефективність, гнучкість, надійність, продуктивність, відмовостійкість.

Практична реалізація даної системи полягає у об’єднанні декілька вузлів в єдине ціле після чого користувач сприйматиме їх як єдину систему. Одним з таких методів є програмне забезпечення Ceph, яке реплікує дані та робить їх відмовостійкими, використовуючи звичайне обладнання та не вимагаючи підтримки спецефічного обладнання. Для того щоб його реалізувати потрібно як мінімум 3 робочі станції на яких буде встановлено віртуальна машина VMware з оперіційними системами GNU/Linux (або на фізичних серверах). Після чого на ОС буде встановлено Nextcloud на основі якого буде працювати розподілена система збору, зберігання та обробки даних.

Висновки

У ході проведення дослідження було реалізовано розподілену систему, яка складається з автономних вузлів, які в свою чергу працюють спільно, створюючи уявлення про роботу в єдиній зв’язній системі.

Перевага даної системи полягає в тому, що логічно об’єднуючи декілька фізично окремих вузлів в одну інформаційну систему вона забезпечує підвищення продуктивності, надійності, відмовостійкості та масштабованості.

к. військ. н. Ясинецький В.П. (НУОУ)
к. військ. н. Кас'яненко М.В. (НУОУ)
к.т.н. Опенько П.В. (НУОУ)
к.т.н. Штаненко С.С. (ВІТІ)

РЕКОМЕНДАЦІЇ ЩОДО ЗАСТОСУВАННЯ GSM МОДУЛЯ ДЛЯ ЗБІЛЬШЕННЯ ДАЛЬНОСТІ ПОВІТРЯНОГО РАДІОЗВ'ЯЗКУ

Єдиним засобом забезпечення управління авіацією (екіпажами) в повітрі є радіозв'язок, який ґрунтується на використанні УКХ діапазону. Вибір УКХ діапазону обумовлений його перевагами перед іншими діапазонами. Однак йому також притаманні і недоліки, найбільш суттєвим з яких є обмежена дальність зв'язку, що не дозволяє забезпечити безперервне управління екіпажами літаків особливо при виконанні бойових завдань на малих та гранично малих висот.

Проведений аналіз відомих способів збільшення дальності повітряного радіозв'язку показав, що вони, з тих чи інших причин, не можуть бути використані в авіації Повітряних Сил ЗС України. Тому виникає нагальна потреба у пошуку та обґрунтуванні рекомендацій щодо збільшення дальності повітряного радіозв'язку.

Більшість держав світу на сьогоднішній день мають добре розвинуту мережу стільникового зв'язку. Цей зв'язок має багаторівневе перекриття за рахунок обслуговування *n*-ої кількості операторів стільникового зв'язку. До того ж він є корпоративний і високотехнологічний, що ускладнює контроль над ним з боку державних структур.

Авторами пропонується створення гібридної радіостанції, шляхом обладнання переносної малопотужної радіостанції авіаційного діапазону частот GSM модулем.

Слід відмітити, що існуючі GSM модулі можливо використовувати не тільки з радіостанціями старого парку вітчизняного виробництва, а і з сучасними радіостанціями різного призначення, наприклад ICOM IC-24 та Harris Falcon III RF-7850.

Функціонально управління екіпажами літаків за допомогою запропонованої гібридної радіостанції можна пояснити наступним чином.

Проведені розрахунки свідчать, що за допомогою запропонованого способу, реалізованому на малопотужній мобільній радіостанції ICOM IC-24 розташованої на висоті 2 м над поверхнею землі, можна забезпечити дальність повітряного радіозв'язку з екіпажами, які виконують завдання на висоті 100 м, до 20 км.

Аналіз запропонованого способу підвищення дальності повітряного радіозв'язку дозволяє визначити його основні переваги та недоліки. До переваг слід віднести:

порівняно велика площа зони управління при невеликих габаритних розмірах;

гнучкість та мобільність використання в особливих випадках організації ПРЗ;

можливість використання GSM модуля з радіостанціями нового і старого парку, які працюють в аналоговому і в цифровому режимі роботи;

не великі габаритні розміри, що дозволяють без особливих зусиль розміщувати гібридну радіостанцію на дахах будівель та інших спорудах, а також здійснювати її маскування;

можливість дистанційного управління гібридною радіостанцією і отримання від неї інформації про поточний стан;

До основних недоліків застосування гібридної радіостанції для ПРЗ можна вважати:

залежність від наявності зони покриття GSM сигналу;

можливість радіоелектронного впливу на GSM мережу або робочу частоту авіаційної радіостанції;

незручності під час забезпечення ПРЗ на території зайнятою противником, а саме, залежність від дій третіх осіб, особливо, під час доставки, розміщення, вмикання та обслуговування гібридної радіостанції.