

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
ВІЙСЬКОВИЙ ІНСТИТУТ
ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ



ХІІІ НАУКОВО-ПРАКТИЧНА
КОНФЕРЕНЦІЯ

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

3 грудня 2020 року

(Доповіді та тези доповідей)

Київ – 2020

У збірнику матеріалів тринадцятої 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

Доповіді

1.	Бовда Е.М., Романюк В.А., Бовда В.Е. Методологічні основи побудови системи управління інформаційно-телекомунікаційними мережами ЗСУ	11
2.	Горбенко І.Д., Потій О.В., Єсіна М.В., Качко О.Г., Олексійчук А.М., Кузнєцов О.О., Горбенко Ю.І. Сутність проблем розробки, стандартизації та застосування перспективних національних стандартів криптографічних перетворень в Україні	22
3.	Гурський Т.Г., Цімура Ю.В., Колодійчук Л.В. Напрямки вдосконалення режиму ппрч у військових засобах радіозв'язку	29
4.	Дерев'янка Я.А., Горбенко І.Д. Вимоги та результати оцінки захищеності перспективного електронного підпису від спеціальних атак	37
5.	Д'яченко А.С., Горбенко І.Д. Параметри та обґрунтованість їх вибору для алгоритму ЕП RAINBOW	43
6.	Каптьол Є.Ю., Горбенко І.Д. Аналіз можливостей та особливості програмування задач криптології на квантовому комп'ютері	49
7.	Кортунов В. І., Вейхай Китай Сучасні системи управління бпла та траєкторне управління	56
8.	Онопрієнко В.В., Малєєва Г.А. Ключова атака відновлення CIRCULANT UOV/RAINBOW	62
9.	Остапчук В.М., Нерознак Є.І., Сова О.Я. Архітектурні рішення для розробки системи зв'язку та інформатизації Збройних Сил України	67
10.	Панченко І.В. Використання новітніх технологій у розробці високотехнологічної зброї	73
11.	Романов О.І., Нестеренко М.М. Побудова транспортної телекомунікаційної мережі Збройних Сил України з урахуванням рекомендацій міжнародного союзу електрозв'язку ITU	77
12.	Шахов Б.С., Єсіна М.В. Аналіз залежності часу виконання криптографічного перетворення від потужності комп'ютера на прикладі алгоритму цифрового підпису PICNIC	83

Тези

1.	Апостол Н.Л., Нерознак Є.І. Модель відмовостійкого сховища даних на базі програмного забезпечення СЕРН	89
2.	Артюх С.Г., Кузьмінський В.С. Алгоритми машинного навчання та їх використання у сфері кібербезпеки	90
3.	Артюх С.Г., Орищук Д.В. Аналіз методик тестування на проникнення мережі VPN спеціального призначення	91
4.	Баканов В.С. Системи аналізу та управління потоками даних	92
5.	Балан А.В., Балан О.А. Особливості системи контролю інформаційних потоків	93
6.	Бернацький А.П., Петрова Д.В. Алгоритм побудови маршруту розвідувального робототехнічного комплексу в умовах невизначеності з використанням штучного інтелекту	95
7.	Бондаренко Л.О., Бузаєва К.О., Руденко В.І., Остапук О.І. Планування місць розгортання підрозділів радіо ретрансляторів на льотно-підйомних засобах	97
8.	Бондаренко Л.О., Коваленко І.Г., Гетьман А.В., Макаруч В.І. Напрямки вдосконалення технологій самоадаптації у мережах КХ радіозв'язку	99
9.	Борисов О.В., Борисов І.В. Забезпечення безпеки резервування інформації в	

	системах розподіленого зберігання даних	101
10.	Бохонько О.В., Нерознак Є.І. Методика організації безпеки мереж зв'язку пунктів управління на основі програмно-апаратних комплексів	103
11.	Бржевська З.М., Кравченко Б.А. Проблематика розвитку інформаційної безпеки в умовах інформаційного протиборства	104
12.	Бункевич К.О., Нестеренко М.М. Програмне забезпечення управління елементами віртуальної мережі на базі протоколу OPENFLOW	106
13.	Василишин В.І., Коваль О.В. Подавлення шуму в мовних сигналах на основі використання методу SSA	107
14.	Вереня М.І., Лазута Р.Г., Власенко О.В. Progressive Web Applications – технологія для створення сучасних клієнт-серверних додатків	108
15.	Войтович М.І., Ліщинська Х.І., Сокіл М.Б., Сеник О.І. Організація спеціалізованих інформаційних систем для підтримки дистанційної освіти	109
16.	Восколович О.І., Колтовсков Д.Г. Використання складних ортогональних сигнально-кодкових конструкцій при побудові заводо захищених каналів управління тактичних БпЛА	110
17.	Гірак П.О. Інтелектуальна мережа мультифункціональних сенсорних вузлів для систем моніторингу та підтримки рішень	112
18.	Глушук В.О., Шелар І.Р., Гелета Д.Р. Підсистема обміну стандартизованими повідомленнями	113
19.	Горбенко В.І., Воронов О.М. Підсистема обліку засобів комп'ютерної техніки навчально-лабораторного комплексу кафедри ВВНЗ	114
20.	Горбенко І.Д., Марухненко О.С., Халімов Г.З. Аналіз можливості використання алгоритму Sphincs+ в інфраструктурі відкритих ключів України	115
21.	Горбенко І.Д., Гармаш Д.В. Криптографічні алгоритми на основі багатовимірних квадратичних перетворень як кандидати на роль основних у постквантовий період	117
22.	Горбенко І.Д., Кандій С.О., Бобух В.А. Генерація загальносистемних параметрів для схеми цифрового підпису dilithium для 5-7 рівнів безпеки	119
23.	Гречишкін Є.В., Кліменко В.М. Підсистема вивчення та визначення вразливостей інформаційних систем умовного противника	121
24.	Гримуд А.Г. Метод ройового управління тактичними безпілотними літальними апаратами	122
25.	Грінков В.О., Грінкова Г.В., Ратаніна О.М. CISCO SECUREX – ефективне рішення безпеки інформаційно- телекомунікаційних систем та серверних додатків	123
26.	Гриценко К.М., Боголій С.М., Нам В.В. Удосконалений метод координатної маршрутизації в мобільних радіомережах з направленими антенами	124
27.	Гук О.М. Перспективи побудови гетерогенних інформаційних систем воєнного призначення з урахуванням концепції NGN (NEXT GENERATION NETWORKS)	125
28.	Гулій В.С., Беляков Р.О. Особливості діагностування та ремонту техніки зв'язку в умовах проведення бойових операцій	126
29.	Гуменюк М.О., Романенко І.І. Шляхи підвищення ефективності застосування безпілотних авіаційних комплексів класу 1 в умовах застосування противником засобів вогневого ураження.	127
30.	Дєдов М.А., Жуков Є.В. Застосування засобів машинного навчання в інформаційних (автоматизованих) системах військового призначення	128
31.	Дмитроца С.С., Нерознак Є.І. Методика реалізації динамічної HONEYPOT-системи на основі контейнерної віртуалізації	129

32.	Добровінський В.П., Лавриненко І.А. Порядок автоматизованого забезпечення даними про метеорологічні умови, для ефективного використання безпілотних авіаційних комплексів і класу	130
33.	Дяченко А.Ю., Троцько О.О. Перспективи використання можливостей прогнозування штучних нейронних мереж у ЗСУ	131
34.	Жилін А.В., Волошин Г.В. Методи та засоби форензики в комп'ютерних мережах	132
35.	Жук О.Г., Кувшинов О.В., Жук П.В. Вибір режиму роботи військових засобів радіозв'язку в умовах складної радіоелектронної обстановки	133
36.	Журавський Ю.В., Шишацький А.В. Комплексна методика управління параметрами військових радіомереж в умовах невизначеності радіоелектронної обстановки	134
37.	Застело Г.І., Цьопко І.Е. Аналіз застосування методу глибокого вивчення штучних нейронних мереж для виявлення кіберзагроз та швидкого реагування на кіберінциденти	135
38.	Зінченко М.О., Макарчук В.І., Атаманенко М.В. Тропосферні станції нового покоління на основі SDR-технології	137
39.	Іов А.О., Макарчук О.М. Імітаційна модель багато процесорної обчислювальної системи зі спільною пам'яттю	138
40.	Калантаєвська С.В., Ільїнов М.Д., Чумак В.К. Розрахунки максимальної дальності зв'язку у радіомережах з повітряними ретрансляторами на БпЛА	139
41.	Калашніков І.А. Актуальність оновлення програмного забезпечення радіостанцій L3HARRIS	140
42.	Калашніков І.А. Багатоканальна універсальна радіостанція L3HARRIS RF-7850D	141
43.	Камчатна К.І., Подоляк О.О., Помін А.Г. Принципи побудови когнітивних радіомереж	142
44.	Каневський Л.Б., Лавриненко О.С., Степанюк Ю.В. Сучасний стан та шляхи розвитку безпілотних авіаційних комплексів класу і для виконання бойових завдань	143
45.	Каневський Л.Б., Наумчак Л.М., Романчук М.П. Формування набору апіорних даних нейромережі генеративною змагальною мережею для автоматизованої обробки аерознімків	144
46.	Каневський Л. Б., Колісник О. С., Романчук М. П. Розроблення прототипу спеціального програмного забезпечення автоматизованої обробки аерознімків для безпілотних авіаційних комплексів Класу 1	145
47.	Катеринчак І.С., Симоненко О.А. Технологія SDN та можливості її впровадження в мережах спеціального призначення	146
48.	Кика І.А., Фесьоха Н.О. Методи візуалізації статистичних даних засобами сучасних веб-застосунків	147
49.	Клименко В.М., Пацкан В.І. Підсистема надання доступу до інформаційного сервісу „Армія FM” в умовах нестабільного з'єднання з мережею на основі кросс-платформеного мобільного додатку розробленого на платформі Flutter	148
50.	Клімович С.О. Варіант оцінки ефективності функціонування системи військового радіозв'язку в умовах радіоелектронного подавлення	150
51.	Коваленко С.В. Аудит інформаційної безпеки – основа ефективного захисту підприємства	151
52.	Коваленко І.Г., Черкасова Ю.О. Застосування технології CAPACITY PLUS MULTI-SITE MOTOTRBO™ для побудови системи транкінгового зв'язку спеціального призначення	153
53.	Коваль М.О. Дослідження ефективності поєднання систем	154

	попередження та виявлення вторгнень	
54.	Ковальчук Л.В., Кучинська Н.В., Теліженко О.Б. Проект стандарту автентифікації, який можна адаптувати для використання в постквантовий період	155
55.	Коровайний Є.О., Нехін М.І., Соболев М.В. Алгоритм побудови маршруту польоту безпілотних літальних апаратів і класу у складних умовах	156
56.	Коротченко Л.А. Аналіз методів підвищення ефективності систем автоматичного керування активних фазованих антен	157
57.	Корченко О.Г. Дрейс Ю.О. Структура удосконалення методу аналізу і оцінювання шкоди національній безпеці України у разі витоку державної таємниці	158
58.	Кравець Т.М., Полець О.П., Пащетник В.І. Особливості геоінформаційних систем що використовуються у сухопутних військах Збройних Сил України	160
59.	Кравченко В.С., Руденко О.В., Доманов І.О., Троцик С.М. Вразливості операційних систем та способи їх детектування	161
60.	Кротов В.Д. Модель управління та розподілу трафіку в радіомережах тактичної ланки управління	163
61.	Кузавков В.В., Михайлюк С.С. Аналіз моделей живучості як властивості системи зв'язку	164
62.	Кулініч Ю.М., Стоюшко А.В., Хомчук В.Я. Перспективи збереження стійкості криптографічних алгоритмів та побудованих на їх основі систем перетворення інформації в умовах стрімкого розвитку квантових комп'ютерів	165
63.	Куниця О.І., Троцько О.О., Дживак П.Б. Аналіз необхідності застосування центрів сертифікації у мережах спеціального призначення	167
64.	Куцаєв В.В. Заходи для блокування дії вірусу шифрувальника в інформаційно-телекомунікаційній системі	168
65.	Лагодний О.В., Павленко В.О., Папуш О.Г. Підхід до класифікації загроз інформації на об'єкті інформаційної діяльності	169
66.	Лазута Р.Р., Прис Г.П., Троцько Л.Г., Макогон О.А. Аналіз умов для впровадження телекомунікаційних стандартів НАТО в Збройних Силах України	170
67.	Ларін В.В., Опенько П.В. Метод обробки відеоінформації в комп'ютерних системах та мережах спеціального призначення	171
68.	Лебідь Є.В. Вдосконалення системи радіочастотної ідентифікації в технології доповненої реальності	172
69.	Левіна М.К., Єсіна М.В. Порівняльний аналіз перспективних електронних підписів на основі алгебраїчних решіток для постквантового періоду	173
70.	Лисенко О.І., Явіся В.С. Концепція побудови системи супутникового зв'язку „Чистий космос”	175
71.	Лисенко О.І., Явіся В.С. Система фіксованого зв'язку на базі кластерів наносупутників	177
72.	Литвинюк Б.В., Воробйов А.О., Шпачинський Є.О., Морозов А.Є., Хижняк І.А. Пропозиції щодо переобладнання машини старшого офіцера батареї управління артилерійським вогнем новітніми засобами зв'язку силами ремонтного підрозділу частини	179
73.	Літвінчук І.С. Основні законодавчі документи з регулювання питань кібербезпеки в Україні та світі	181
74.	Лоза В.В. Реорганізація інформаційно-телекомунікаційних систем в умовах кібервпливу із застосуванням нейромережевої технології	183
75.	Любарський С.В., Горбенко С.І. Підвищення ефективності системи геопросторового обліку та контролю земель та іншого нерухомого військового (державного) майна МОУ	184

76.	Мазулевський О.Є., Недовба К.С. Аналіз програмного забезпечення запобіганню витоку інформації з інформаційно-телекомунікаційних мереж	185
77.	Мазулевський О.Є., Саченко А.П. Варіант застосування систем запобігання вторгнень в ІТС у Збройних Силах України	186
78.	Макарчук М.М., Кузенков В.С. Розпізнавання комп'ютерних вірусів за допомогою нейронних мереж	187
79.	Маліновський Н.О., Голушко С.Л., Позігун С.А. Оптимізація роботи системи відеоспостереження на пунктах управління під час виконання операцій (бойових дій)	188
80.	Мартинчик І.А., Нерознак Є.І. Методи маршрутизації трафіку в сенсорних мережах з використанням елементів штучного інтелекту	189
81.	Мартинюк В.В., Паламарчук Н.А., Паламарчук С.А., Черниш Ю.О. Деякі задачі з вдосконалення інформаційної та кібернетичної безпеки об'єктів критичної інфраструктури	190
82.	Масесов М.О., Іващенко Є.В. Розвиток штучних систем спеціального призначення для розпізнавання образів	191
83.	Масесов М.О., Погребний Д.В., Новицький Д.В. Перспективи впровадження сучасних телекомунікаційних технологій у засобах тропосферного зв'язку	192
84.	Мілевський Б.В. Методи підвищення стійкості криптографічних протоколів системи електронного документообігу до квантових атак	193
85.	Міна С.В., Нерознак Є.І. Модель відмовостійкого кластера віртуалізації з можливістю „гарячої” міграції віртуальних машин	194
86.	Місевич К. С. Технологія забезпечення кібербезпеки хмарного середовища на базі рішення CISCO CLOUDLOCK	195
87.	Могилевич Д.І., Кононова І.В. Аналіз моделей оцінки та методів підвищення надійності програмного забезпечення систем управління військами та озброєнням	196
88.	Мороз А.А., Грінков В.О. Перспективи та можливості застосування підсистеми визначення стійкості системи збереження даних	199
89.	Мотчаний А.С., Здоренко Ю.М., Легкобит В.С. Підсистема аналітичної обробки даних відеопотоку на основі методів машинного навчання	200
90.	Нестеренко М.М., Артамошенко Є.С., Ворожко А.М. Програмно-апаратний комплекс розпізнавання військової техніки при обробці відеопотоку на базі NVIDIA JETSON NANO	201
91.	Нестеренко М.М., Кондратюк А.Г., Сінчук В.В. Підсистема взаємодії з користувачем системи обліку матеріальних засобів лабораторії ТЗН ВВНЗ	202
92.	Нестеренко М.М., Ошурко В.М., Бункевич К.О. Програмне забезпечення управління елементами віртуальної мережі на базі протоколу OPENFLOW	204
93.	Нестеренко М.М., Плужник І.І., Шрамко О.В. Програмне забезпечення виявлення сервісів для балансування HIGH-LOAD систем на основі технології DOCKER SWARM	205
94.	Нестеренко М.М., Теслов Д.С., Успенський О.А. Підсистема оптимізації etl процесів на основі алгоритму кластеризації <i>K-means</i> комплексу спеціалізованого програмного забезпечення „платформа низового моніторингу об'єктів будівництва міністерства оборони України „GROUND CONTROL””	207
95.	Нестеренко М.М., Фесьоха Н.О., Гнесь О.О. Підсистема оцінки продуктивності IP PBX при використанні різних типів віртуалізації	208
96.	Оверчук С.П., Бедрій Н.А. Підходи щодо вибору і налаштування сервоприводів для безпілотних літальних апаратів класу 1 з урахуванням потреб і досвіду Операції об'єднаних сил	209
97.	Ольшанський В.В., Гурський Т.Г., Поляк І.Є. Методика вибору значень	210

	параметрів сигналів з пррч в умовах радіоелектронного подавлення	
98.	Остапчук В.М., Сова О.Я. Динамічна модель радіоелектронного конфлікту з урахуванням можливостей сторін	211
99.	Острианська Є.В., Єсіна М.В., Горбенко Ю.І. Відомі атаки на схему цифрового підпису FALCON	212
100.	Павелко Є.І. Підвищення сталості функціонування мережі цифрового транкінгового зв'язку спеціального призначення Збройних Сил України шляхом впровадження технології CAPACITY PLUS MULTI-SITE	214
101.	Палиця В. О., Шакович Н.В., Горбачевський С.К., Орда М.В. Система інформаційного забезпечення військової освіти з питань оцінювання результатів навчання випускників ВВНЗ за підсумками їх службової діяльності	216
102.	Палівода В.С., Хоменко П.В., Березанський Д.О. Перспективи застосування радіостанцій з широкосмуговою адаптивною мережевою формою сигналу в Збройних Силах України	217
103.	Пантась І.О., Масесов М.О. Аналіз методів підвищення живучості телекомунікаційних мереж зв'язку	219
104.	Пархоменко Д.О., Захарченко В.В. Метод автоматизації процесу вибору маршруту польоту безпілотної літальної апаратури при проведенні повітряної розвідки	220
105.	Піскун О.М., Медіна М.С., Медіна О.В. Обґрунтування створення системи моніторингу ГНСС сигналів	221
106.	Погребняк Л.М., Висоцька Т.М. Аналіз методів зменшення Пік-фактору в системах безпроводового широкосмугового доступу	222
107.	Погребняк С.В. Проблематика діагностування новітніх систем телекомунікаційного обладнання	223
108.	Постник Ю.А., Артюх С.Г. Аналіз реалізації фішингових атак на мережу ІСД-інтернет	224
109.	Прийма О.О., Чевардін В.Є., Пономарьов О.А. Оцінка швидкодії програмних функцій скалярного множення з використанням MIRACL CRYPTOGRAPHIC SDK	225
110.	Проскуровський Р.В. Актуальні питання кібербезпеки України	226
111.	Прядка О.С., Нерознак Є.І. Модель застосування серверних систем в концепції інтернету військових речей (IOBT)	228
112.	Радченко М.М., Драглюк О.В., Коротков М.М., Бригадир С.П., Маланчук М.Ф. Особливості систем оборонного планування в США та в Україні	229
113.	Редзюк Є.В., Дрига Д.В., Стемпковська Я.А. Інтерактивна платформа тестування військовослужбовців на основі серверу додатків TOMCAT	233
114.	Редзюк Є.В., Румша Д.С. Модуль реєстрації, автентифікації та авторизації за допомогою стандарту OAuth2 користувача комплексу спеціалізованого програмного забезпечення „Платформа низового моніторингу об'єктів будівництва Міністерства Оборони України „GROUND CONTROL””	234
115.	Рожко С.Ю., Слюсар П.П., Довбенко О.В., Дворський М.В. Аналіз програмних додатків щодо вирішення завдань технічного аналізу радіотехнічних сигналів	235
116.	Романенко М.М. Спосіб реєстрації діагностичної інформації для контролю технічного стану радіоелектронного обладнання	236
117.	Самойлов І.В., Дорошенко Д. В., Толстих В.А. Варіант побудови нечітких відношень для оцінки захищеності інформаційних систем	238
118.	Самчишин О. В., Охрімчук В.В. Метод побудови шаблонів потенційно небезпечних кібератак	239
119.	Сеник А.П., Білаш О.В., Ліщинська Х.І., Войтович М.І. Застосування	241

	інформаційних технологій для організації систем спеціалізованих консультацій	
120.	Семенякіна В.С., Єсіна М.В. Дослідження та аналіз кандидату на перспективний постквантовий електронний підпис FALCON	242
121.	Сипливець С.В., Нерознак Є.І. Модель сервера віртуалізації на основі технологій контейнеризації	246
122.	Сінчук В.В., Нестеренко М.М., Успенський О.А. Підсистема взаємодії з користувачем системи обліку матеріальних засобів лабораторії ТЗН ВВНЗ	247
123.	Сінько В.В., Могилевич В.Д. Аналіз факторів, які впливають на надійність програмного забезпечення інформаційних систем спеціального призначення	248
124.	Слюсар В.І. ROS-M та програмна архітектура AGVRA	249
125.	Слюсар В.І. Тензорно-матричні основи теорії штучного інтелекту	251
126.	Слюсар В.І. Стратегія стандартизації у СФЕРІ UGV	253
127.	Сова М.В., Олексенко В.П. Концепція кібербезпеки Збройних Сил США	254
128.	Совік О.В., Сергієнко А.В. Розподіл частотного ресурсу сучасних широкосмугових станцій в тактичній ланці управління Збройних Сил України	255
129.	Солодовник В.І., Чуйко В.В. Способи підвищення енергетичної ефективності засобів військового радіозв'язку з підтримкою технології MIMO	256
130.	Степаненко Є.О., Симоненко О.А. Математична модель прогнозування радіозв'язності вузлів в радіомережах класу MANET	258
131.	Стоцький І.В., Сонько М.М. Підсистема автоматизації роботи куратора навчальної групи ВВНЗ на основі мобільного додатку	259
132.	Сусь Б.А., Грохольський Я.М., Лиманська О.Л. Особливості завадостійкого кодування при переході через ймовірнісну межу $P \geq 10^{-2}$	260
133.	Ткаченко І.М., Величко В.П. Аудит стану кіберзахисту, як складова оцінки кіберзахисту об'єктів критичної інфраструктури з урахуванням індикаторів кіберзагроз	263
134.	Толкунова О.А., Симоненко О.А. Модель передачі інформації в мережах спеціального призначення на основі протоколу QUIC	264
135.	Троцько О.О. Імітаційне моделювання процесу передачі повідомлень у каналах зв'язку з високошвидкісними об'єктами за умов нелінійного доплерівського зсуву частоти	265
136.	Троянський В.О., Застело Г.І. Моделювання процедури оцінювання захищеності інформаційно-телекомунікаційної системи від кібератак	267
137.	Труш О.В., Мягкова Л.А., Труш І.О. Забезпечення цілісності інформації в інформаційно-телекомунікаційних системах спеціального призначення	268
138.	Фесенко О.Д., Беляков Р.О., Радзівілов Г.Д. Методика керування траєкторією БпЛА в автономному режимі польоту на основі нейромережевого алгоритму MELM – MADGWICK	270
139.	Фесенко Д. О., Горбенко І. Д. Використання децентралізованих технологій для засобів автентифікації автомобіля	271
140.	Фесьоха Н.О., Лейник Д.М. Модуль централізованого зберігання та обробки даних інформаційної системи технічного обслуговування абонентів служб технічної підтримки	274
141.	Фесьоха В.В., Фесьоха Н.О., Доброштан О.С. Автентифікація користувача інформаційної системи на основі поведінкової біометрії із використанням нечіткої логіки	275
142.	Фриз С.П., Кальватинський О.В., Авсієвич Р.О. Модель інтегрованої системи моніторингу надводної обстановки в межах виключної (морської) економічної зони України	276
143.	Фтемов Ю.О. Рекомендації зі створення спеціалізованого програмного забезпечення для розрахунку системи інженерних загороджень	277

144.	Хлапонін Ю.І., Козубцов І.М., Козубцова Л.М. Проблема кібербезпеки в освітніх інформаційних системах та інформаційних технологіях	279
145.	Хмуляк І. В. Використання окремої категорії програмного забезпечення в інформаційно-телекомунікаційних системах для організації зв'язку	280
146.	Хусаїнов П.В., Петров В.О. Напрямки застосування інтелектуального аналізу даних для виявлення новітніх кібератак	282
147.	Хусаїнов П.В. Проблематика підтримки прийняття рішень оперативного реагування на кіберінциденти	283
148.	Цуканов О.Ф., Якорнов Є.А. Протидія „Рою” безпілотних літальних апаратів противника	284
149.	Чевардін В.Є., Бондарчук В.О., Сівоха О.М. Методи та інструменти тестування на проникнення Web-додатків	286
150.	Чевардін В.Є., Лаврик І.В. Перспективні напрямки розвитку методів криптографічного захисту інформації	287
151.	Чевардін В.Є., Штобза Д.В. Лабораторний стенд детектування WiFi точок доступу	288
152.	Черешня В.Р., Курдеча В.В., Скулиш М.А. Вдосконалений метод активації Веб-сервісів на основі безсерверних хмарних обчислень	289
153.	Чупілко О.І., Курдеча В.В., Суліма С.В. Модифікований спосіб міжмашинного зв'язку для мережі Інтернету речей	291
154.	Чухломін В.В., Грохольський Я.М. Модель захищеної мережевої архітектури на мобільних вузлах з використанням протоколів MIP та MIPv6	293
155.	Шацький І.О. Комбінаторна M-FSK модуляція в декаметровому діапазоні хвиль	294
156.	Юнгін М.А. Грінков. В.О. Розробка системи розпізнавання зображень на основі апарату штучних нейронних мереж	295
157.	Яровий В.С., Радзівілов Г.Д. Новітній підхід до діагностики несправностей випрямних трансформаторів високочастотних джерел живлення	296

МЕТОДОЛОГІЧНІ ОСНОВИ ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИМИ МЕРЕЖАМИ ЗСУ

Інформаційно-телекомунікаційні мережі (ІТМ) ЗСУ мають в своєму складі велику кількість підсистем різного функціонального призначення та застосування. Такі системи потребують якісного управління. Інформаційно-телекомунікаційні мережі (ІТМ) ЗСУ будуються під завдання, які потрібно вирішувати, а відповідно система управління ними повинна забезпечувати багаторівневу підтримку прийняття рішень посадовими особами по ефективному управлінню ІТМ для забезпечення планування, підготовки до застосування за призначенням, застосування і відновлення ІТМ і боєздатності сил (засобів), а також бойового застосування військ зв'язку з виконанням вимог до стійкості, безперервності, оперативності та скритності.

Існуючі зараз технології управління інформаційно-телекомунікаційними мережами розраховані на статичні або квазістатичні умови їх функціонування та враховують особливості, що характерні для цивільних систем. Відмінностями між цивільними та військовими системами управління мережами полягають в наступному: різні цілі, етапи, функції, рівні управління, вимоги до оперативності управління, інтенсивність зовнішнього впливу дестабілізуючих факторів (вогневе враження, активні завади, радіоелектронна та інформаційна боротьба тощо), тобто, у військових системах зв'язок повинен бути за будь-яких умов. На сьогодні склалася така ситуація, що в Збройних Силах України немає ефективної автоматизованої системи управління ІТМ. Всі до цього намагання створити такі системи стиналися з величезною кількістю труднощів організаційного та технологічного характеру. Підвищення ефективності використання ресурсів ІТМ, ефективне виконання завдань може бути досягнуто за рахунок розвитку і вдосконалення системи управління зв'язком ЗСУ, в першу чергу за рахунок її автоматизації.

Проведений аналіз дозволяє зробити висновок, що всі проведені до цього дослідження не враховували зовнішній вплив та високу динаміку зміни станів ІТМ. Тому, в основу побудови системи управління ІТМ повинно максимально використати принципи застосування системного підходу. Тоді схема побудови ІТМ буде складатися з наступних етапів: визначення вихідних даних; визначення цілей функціонування ІТМ та СУ; визначення етапів та цілей управління мережами; визначення функцій та задач управління мережами; визначення моделей, алгоритмів управління та критеріїв оцінки ефективності СУ; визначення варіантів реалізації СУ та вибір раціонального (оптимального) варіанту СУ. В подальшому провести на основі критеріїв оцінки ефективності вибір оптимального варіанту побудови системи управління.

1. Вихідні дані та цілі функціонування.

Перспективна ІТМ складається з системи управління телекомунікаційними мережами (СУ ТКМ) та телекомунікаційних мереж (ТКМ) (рис. 1). На ці дві складові системи постійно впливають зовнішнє середовище та супротивник (E), що безпосередньо виявляється в вигляді бойового застосування військ, вогневого враження, радіоелектронної боротьби.

Телекомунікаційні мережі $s = 1 \dots S$ мають головною метою Z^S – передача інформації між органами військового управління з заданими параметрами. ТКМ складаються з наступних мереж: проводового зв'язку, радіозв'язку, радіорелейного зв'язку, тропосферного зв'язку, супутникового зв'язку, оптоелектронного зв'язку. Всі вони описуються наступними характеристиками, що в кінцевому випадку визначають вихідні дані мереж $\{X_{js} = X_{1s}, X_{2s}, X_{3s}, X_{4s}, X_{5s}, X_{6s}, X_{7s}\}$: параметри мережі: кількість вузлів, розміщення на місцевості, ступінь покриття території мережею, кількість базових станцій, час функціонування мереж, протоколи інформаційного обміну у відповідності з еталонною моделлю OSI , тощо $\{X_{1s}\}$;

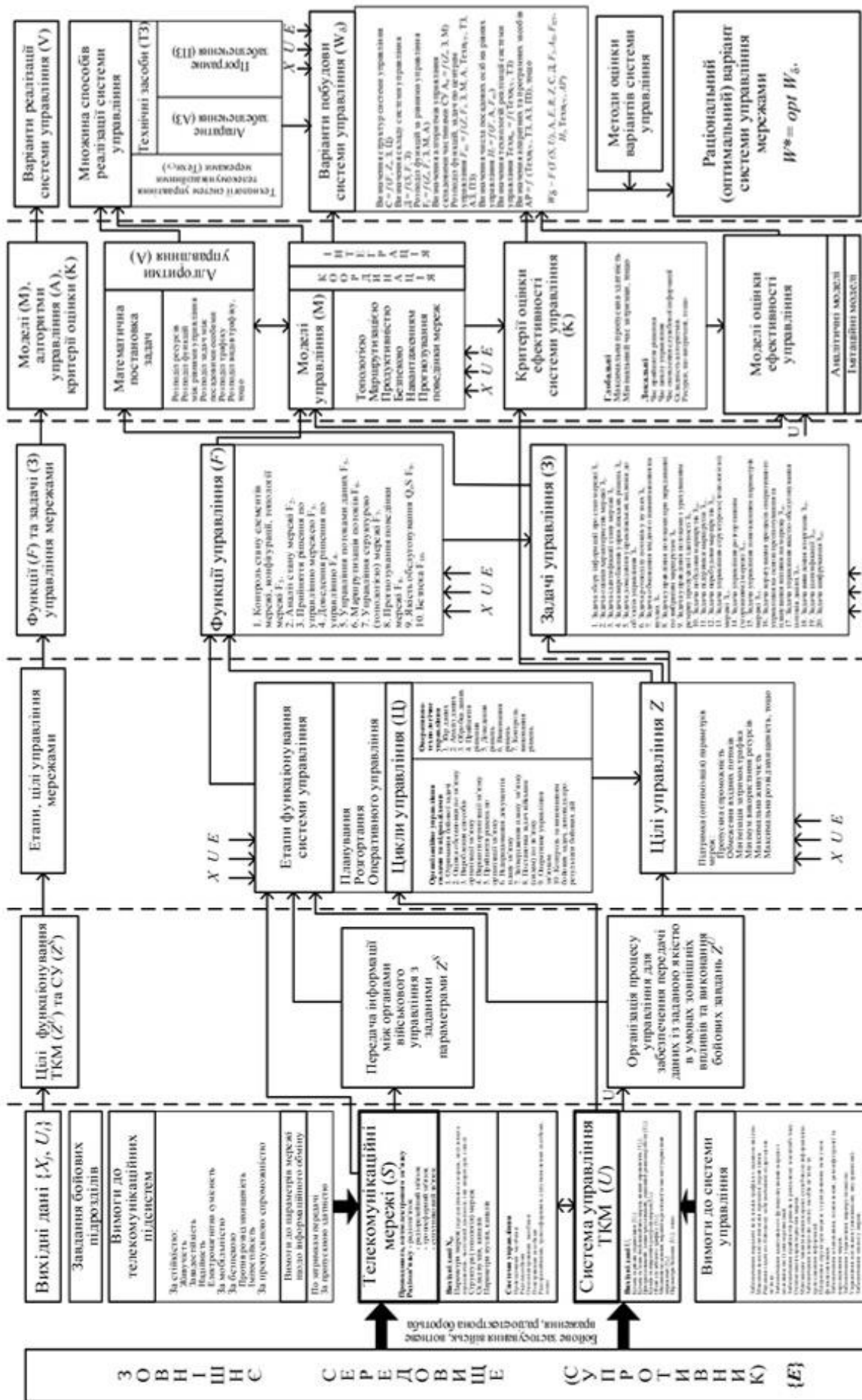


Рис. 1. Схема синтезу системи управління телекомунікаційною мережею (ТКМ)

структура (топологія) мереж $\{X_{2S}\}$;
склад вузлів $\{X_{3S}\}$, каналів $\{X_{4S}\}$ (тип апаратури, обладнання; тип трафіку; рівень управління; кількість радіостанцій та їх типи, тощо);
навантаження (тип, максимальне значення) $\{X_{5S}\}$, тощо;
параметри вузлів $\{X_{6S}\}$, каналів $\{X_{7S}\}$ (пропускна спроможність; кількість абонентів, що обслуговуються; потужність передавачів; частотний діапазон; алгоритми управління, тощо).

Разом з тим, кожна з цих мереж має свою систему управління – проводовими засобами, радіозасобами, оптоелектронними засобами, повітряними засобами, радіорелейними, тропосферними, супутниковими засобами.

Елементами та об'єктами управління ТКМ є: окремі мережі, зони, напрями, маршрути, вузли, канали, радіостанції, маршрутизатори, комутатори, шлюзи, телекомунікаційні платформи, сервера, АРМи посадових осіб, тощо.

До телекомунікаційних мереж пред'являються наступні вимоги [1]:

1. За стійкістю: живучість, завадостійкість, надійність, електромагнітна сумісність.
2. За мобільністю.
3. За безпекою: протирозвід захищеність, імітостійкість.
4. За пропускною спроможністю.

В процесі експлуатації телекомунікаційних мереж до параметрів передачі даних (рекомендації міжнародного союзу електрозв'язку – сектор телекомунікацій *ITU-T*) пред'являють вимоги до [2]: затримок передачі інформації; швидкості передачі даних; імовірності помилок в пакетах; пропускної здатності мережі, тощо.

В основу синтезу СУ ТКМ покладено агрегативно-декомпозиційний підхід, що дозволяє представити майбутню систему у вигляді сукупності взаємопов'язаних елементів різного рівня деталізації [3]. Цей підхід включає послідовну декомпозицію цілей, функцій, задач, що виконуються системою та агрегування на відповідному рівні деталізації елементів для генерування варіантів побудови системи на рівні деталізації, що розглядається. В подальшому будемо використовувати цей підхід.

Система управління U телекомунікаційними мережами (ТКМ) має глобальну мету Z^U – забезпечення передачі даних із заданою якістю в умовах зовнішніх впливів та виконання бойових завдань.

До системи управління телекомунікаційною мережею пред'являються наступні вимоги [4, 5]:

1. Забезпечення передачі всіх видів трафіка з заданою якістю.
2. Максимальна автоматизація процесів управління.
3. Рішення задач по бойовому забезпеченню підрозділів зв'язку.
4. Забезпечення адаптивного функціонування мережі з можливістю її самоорганізації.
5. Забезпечення прийняття рішень в реальному масштабі часу.
6. Оптимізація характеристик мереж.
7. Мінімальне завантаження мережі службовою інформацією.
8. Забезпечення контролю стану засобів зв'язку та проходження інформації.
9. Підтримка структури (топології) мереж з урахуванням змін умов функціонування.
10. Забезпечення планування, поновлення, реконфігурації та нарощування мереж.
11. Забезпечення управління маршрутизацією.
12. Управління потоками (зовнішніми, внутрішніми).
13. Забезпечення захисту мереж, тощо.

Вихідними даними для системи управління телекомунікаційною мережею мають бути наступні дані $U = \{U_i\}, i = \overline{1, T}$:

1. Кількість рівнів управління $\{U_1\}$.
2. Кількість телекомунікаційних мереж, якими управляють $\{U_2\}$.
3. Централізований, децентралізований, змішаний режими роботи $\{U_3\}$.

4. Кількість апаратних та програмних ресурсів мереж $\{U_4\}$.
5. Обсяг службового трафіку $\{U_5\}$.
6. Множина можливих варіантів реалізації технології управління мережами $\{U_6\}$.
7. Параметри безпеки $\{U_7\}$, тощо.

2. Етапи, цілі управління мережами.

Етапами функціонування системи управління є планування, розгортання (організаційні способи реалізації) і оперативного управління (організаційно-технологічний спосіб).

Етап планування здійснюється центром управління мережі. Сутність планування полягає в організації діяльності органу управління, яка направлена на формування і прийняття рішення по організації мережі (способи побудови мережі), своєчасну розробку документів і доведення їх до підлеглих (постановка задач перед силами зв'язку та розподіл сил та засобів [4, 5]).

Система управління повинна реалізовувати наступні види управління зв'язком: *організаційне, організаційно-технологічне і технологічне* [4, 5].

1. На рівні *організаційного управління* повинні реалізовуватися цільові завдання функціонування системи зв'язку шляхом планування зв'язку, управління побудовою системи зв'язку і бойовим застосуванням з'єднань і частин зв'язку.

Завдання планування при управлінні мережами являють собою процес постановки цілей, які потребують досягнення і розробки програми їх досягнення, оформленої у вигляді сукупності документів по зв'язку, основним з яких є план зв'язку. Змістом процесу планування є розподіл ресурсів мереж і визначення порядку їх використання. Сутність і зміст планування зв'язку визначається її цільовим призначенням, характером функціонування та принципами застосування в той або іншій обстановці.

Завдання планування розбиваються на групи: для стаціонарного та мобільного компоненти, для радіозв'язку, для радіорелейного, для тропосферного та космічного зв'язку, для вузлів зв'язку та ліній прив'язки, для мереж доступу.

Наявність мобільних компонент, а також поточні зміни в топології мереж і систем управління, призводять до необхідності перерозподілу функцій управління зв'язком по ланках і рівнях управління АСУ, а також відповідного уточнення складу і взаємозв'язку завдань, що вирішуються посадовими особами при управлінні мережами.

При цьому завдання автоматизованого управління зв'язком на організаційному рівні повинні вирішуватися на основі застосування комплексів засобів автоматизації управління зв'язком, загального програмного забезпечення, спеціального програмного забезпечення організаційного управління та елементів інформаційного забезпечення – баз даних організаційного управління, реалізованих на основі сучасних засобів прикладної середовища систем підтримки прийняття рішень (далі СППР).

При цьому в загальному випадку перспективні СППР, що реалізуються в АСУЗ, як пасивні, так і активні, можуть поєднувати методи інформаційного пошуку, інтелектуального аналізу даних, пошуку знань в базах даних, міркувань на основі прецедентів, імітаційного моделювання, генетичних алгоритмів, нейронних мереж та ін. в залежності від конкретних завдань, і будуватися на основі технології аналітичної обробки інформації в реальному часі (*OLAP – online analytical processing*) і варіантів її реалізації.

Для безпосереднього вирішення завдань організаційного управління зв'язком на організаційному рівні управління повинні виділятися наступні основні логічні підсистеми:

підсистема обліку даних обстановки по зв'язку;

підсистема моделювання функціонування мереж зв'язку;

підсистема планування зв'язку;

підсистема планування застосування елементів системи зв'язку (вузлів, центрів, ліній, мереж,

системи технічного забезпечення зв'язку і АСУ, резерву сил і засобів зв'язку та автоматизації);

підсистема оперативного управління зв'язком;

підсистема забезпечення оперативно-технічної служби на елементах системи зв'язку;
підсистема всебічного забезпечення функціонування системи зв'язку.

2. На рівні **організаційно-технологічного управління** повинні вирішуватися завдання по управлінню мережами і послугами зв'язку у взаємодії з підсистемами організаційного та технологічного управління.

Для вирішення завдань організаційно-технологічного управління зв'язком на відповідному рівні управління повинні виділятися наступні основні логічні підсистеми:

підсистема управління якістю надання видів і послуг зв'язку,
підсистема контролю стану і зміна структури мереж зв'язку.

Основу технічної реалізації даного рівня повинен становити комплекс засобів автоматизації оперативно-технічного управління мережами зв'язку, що включає:

автоматизовані робочі місця посадових осіб, об'єднані локальною обчислювальною мережею з серверами додатків, і бази даних;

програмне та інформаційне забезпечення, що забезпечує автоматизоване рішення задач оперативно-технічного управління.

3. На рівні **технологічного управління** повинні вирішуватися завдання контролю і зміни технічного стану засобів зв'язку (мережових елементів) мереж зв'язку шляхом створення відповідної підсистеми.

Технологічне управління зв'язком здійснюється з використанням можливостей сучасних засобів зв'язку сприймати керуючі команди і сигнали з боку АСУЗ, змінювати під їх впливом свої стани, а також видавати в АСУЗ інформацію про свій стан.

Для управління зв'язком і військами зв'язку в різних умовах обстановки може організовуватися шляхом створення окремих мереж управління (службового зв'язку) або шляхом використання каналного ресурсу мереж зв'язку.

На мережу управління покладаються завдання по передачі командної інформації, передачі даних, передачі команд технологічного управління комплексами технічних засобів системи зв'язку ЗСУ, управління рухомими одиницями тощо. Виконання даних завдань може забезпечуватися за рахунок створення відповідних підсистем мережі управління.

Крім цього в АСУЗ повинна створюватися підсистема безпеки функціонування, яка спрямована на забезпечення схоронності даних, що циркулюють в системі, розмежування доступу посадових осіб органів управління зв'язком до інформації, їх аутентифікацію і недопущення несанкціонованого втручання.

Етап розгортання полягає в розгортанні мережі в заданому районі. При цьому задачі етапу розгортання (перепланування) мережі можуть виконуватися й на етапі оперативного управління при значних її змінах (ушкодженні, введенні нових угруповань військ й ін.). Контроль за етапом розгортання мережі здійснюється із центру управління мережею.

На етапі оперативного управління за прийнятими критеріями ефективності постійно оцінюється стан мереж, і приймаються міри (відповідно до плану та реальної обстановки) по втриманню показників ефективності функціонування в заданих межах або здійснюється їх системна (користувальницька) оптимізація.

Задачі оперативного управління (на відмінність задач планування) вирішуються змішаним способом (централізовано/децентралізовано) у режимі реального часу, а за змістом багаторазово їх повторюють. Цикл управління (Ц) мережі здійснюється органом управління (особою, що приймає рішення) та включає (див. рис. 1) [5, 6]:

– **збір інформації про стан мережі** (при цьому необхідно приймати рішення за об'ємом, типом, рівнями, функціями збору службової інформації);

– **аналіз даної інформації та її обробка** – визначаються: ступінь виконання мережею своїх функцій, необхідність управляючого впливу, цілі управління з подальшою деталізацією їх на підцілі;

– **прийняття рішення** (реконфігурація мережі, перерозподіл каналів транспортної мережі та мережі доступу, маршрутизація та обмеження потоків, оновлення елементів мережі тощо);

– **доведення та виконання рішення** (видача та доведення управляючих команд, розсилання службової інформації, резервування ресурсу, налаштування обрання, встановлення потужності передавачів, спрямованість антен тощо);

– **контроль виконання рішень** у задані часові інтервали.

Цілями системи управління (Z^U) (рис. 1) можуть бути екстремум або підтримка (виступають як обмеження) заданих параметрів функціонування всієї мережі або її елементів (зона, напрямок, маршрут, вузол, канал), що можна представити в вигляді [4, 5]:

$$Z^U = f(C, P^e, P^{зв}, F, Y^{CY}, O, R) \rightarrow opt$$

при обмеженнях $R \leq R_{доп}$ та $O \leq O_{доп}$, $\{T_{ц} \leq T^{доп}\} \rightarrow min$

де C – структура системи управління;

P^e – множина параметри елементів системи управління;

$P^{зв}$ – множина параметрів зв'язків між елементами системи управління;

F – сукупність функцій, що реалізуються системою управління ТКМ;

Y^{CY} – умови функціонування системи управління;

O – обмеження на значення характеристик властивостей системи управління, що створюється;

R – обмеження на ресурси, за допомогою яких буде синтезуватися система управління;

$T_{ц}$ – час циклу оперативного управління мережею;

$T^{доп}$ – час, що відведений на управління мережею або її етапи, який визначається директивними документами.

Разом з тим, у системі управління мережею існує ієрархія цілей Z^U . Загальна ціль поділяється на підцілі: планування та оперативного управління. Оперативне управління в свою чергу поділяється на управління якістю обслуговування, конфігурацією, несправностями, ресурсами тощо. В загальному випадку Z^U можна представити у вигляді списків підцілей, які пов'язані визначеними відношеннями [6, 7]:

$$Z^U = \{Z_0 \theta_{01} \{Z_{11}, Z_{12}, \dots, Z_{1n}\} \theta_{12} \{Z_{21}, Z_{22}, \dots, Z_{2n}\} \dots \theta_{ij} \{Z_{k1}, Z_{k2}, \dots, Z_{kn}\}\},$$

де Z^U – ієрархія цілей системи управління; Z_0 – глобальна ціль; Z_{ij} – i -а підціль j -го рівня ієрархії цілей, $i = \overline{1, I}$; $j = \overline{1, J}$; θ – множина відношень на підцілі ієрархії цілей.

Наприклад, до мережевих (зонових) цілей управління можна віднести оптимум наступних параметрів $Z = \{Z_1, Z_2, \dots, Z_n\}$:

Z_1 – продуктивність всієї мережі, мережі певного рівня або її зони, напряму, маршруту, каналу; Z_2 – потужність радіопередавачів мережі чи її зони; Z_3 – ступінь покриття території (абонентів) мережею (аероплатформами); Z_4 – структурна надійність (зв'язність) мережі, її зони; Z_5 – кількість апаратних ресурсів (аероплатформ, базових станцій, серверів тощо); Z_6 – час функціонування мережі її зони, напряму, маршруту; Z_7 – обсяг службового трафіка; Z_8 – час планування, розгортання, відновлення мережі чи її зони, напряму; Z_9 – параметри безпеки й т. д.

3. Функції та задачі управління мережами.

Система управління ТКМ повинна забезпечити виконання основних функцій $F = \{F_{\xi}\}$, $\xi = \overline{1, \xi}$, як в циклі управління так окремі функції.

Цикл управління складається з функцій:

1. Контроль стану елементів мережі, конфігурації, топології мережі F_1 .
2. Аналіз стану мережі F_2 .
3. Прийняття рішення по управлінню мережею F_3 .
4. Доведення рішення по управлінню F_4 .

Окремі функції, що безпосередньо не входять до циклу управління.

5. Управління потоками даних F_5 .
6. Маршрутизація потоків F_6 .
7. Управління структурою (топологією) мережі F_7 .
8. Прогнозування поведінки мережі F_8 .
9. Якість обслуговування QoS F_9 .
10. Безпека F_{10} , тощо.

На систему управління мережею покладаються наступні задачі $Z = \{Z_\eta\}, \eta = \overline{1, \eta}$:

1. Задача збору інформації про стан мережі Z_1 .
2. Задача оцінки характеристик мережі Z_2 .
3. Задача ідентифікації стану мережі Z_3 .
4. Задача вироблення управлінських рішень Z_4 .
5. Задача доведення управлінських впливів до об'єктів управління Z_5 .
6. Задача розподілу потоків у вузлах Z_6 .
7. Задача обмеження вхідного навантаження на вузлах Z_7 .
8. Задача управління потоками при передаванні по вибраним маршрутам Z_8 .
9. Задача управління потоками з урахуванням резерву пропускної здатності Z_9 .
10. Задача побудови маршрутів Z_{10} .
11. Задача підтримки маршрутів Z_{11} .
12. Задача перебудови маршрутів Z_{12} .
13. Задача управління структурою (топологією) мережі Z_{13} .
14. Задача управління розгортанням (згортанням) мережі Z_{14} .
15. Задача управління поновленням параметрів мережі Z_{15} .
16. Задача корегування процесів оперативного управління на основі прогнозування та планування впливів на мережу Z_{16} .
17. Задача управління якістю обслуговування потоків даних Z_{17} .
18. Задача виявлення вторгнень Z_{18} .
19. Задача ідентифікації Z_{19} .
20. Задача шифрування Z_{20} , тощо.

Функції та задачі управління мережами визначають майбутню логіку роботи СУ ТКМ на всіх етапах функціонування (див. табл. 1). При виконанні кожної функції управління можливе вирішення однієї або кількох задач управління.

Таблиця 1

№ з/п	Функції управління	Задачі управління
1	Контроль стану елементів мережі, конфігурації, топології мережі F_1 .	Задача збору інформації про стан мережі Z_1 (для всіх функцій управління).
2	Аналіз стану мережі F_2 .	Задача оцінки характеристик мережі Z_2 . Задача ідентифікації стану мережі Z_3 .
3	Прийняття рішення по управлінню мережею F_3 .	Задача вироблення управлінських рішень Z_4 .
4	Доведення рішення по управлінню F_4 .	Задача доведення управлінських впливів до об'єктів управління Z_5 .
5	Управління потоками даних F_5 .	Задача розподілу потоків у вузлах Z_6 . Задача обмеження вхідного навантаження на вузлах Z_7 . Задача управління потоками при передаванні по вибраним маршрутам Z_8 . Задача управління потоками з урахуванням резерву пропускної здатності Z_9 .
6	Маршрутизація потоків F_6 .	Задача побудови маршрутів Z_{10} . Задача підтримки маршрутів Z_{11} .

		Задача перебудови маршрутів Z_{12} .
7	Управління структурою (топологією) мережі F_7 .	Задача управління структурою (топологією) мережі Z_{13} . Задача управління розгортанням (згортанням) мережі Z_{14} . Задача управління поновленням параметрів мережі Z_{15} .
8	Прогнозування поведінки мережі F_8 .	Задача корегування процесів оперативного управління на основі прогнозування та планування впливів на мережу Z_{16} .
9	Якість обслуговування QoS F_9 .	Задача управління якістю обслуговування потоків даних Z_{17} .
10	Безпека F_{10} .	Задача виявлення вторгнень Z_{18} . Задача ідентифікації Z_{19} . Задача шифрування Z_{20} .

4. Моделі, алгоритми управління, критерії оцінки ефективності системи управління, моделі оцінки ефективності управління.

На основі визначених функцій $\{F\}$, задач управління $\{Z\}$ здійснюється їх математична постановка та визначаються методи рішення. Для цього може використовуватися математичний апарат теорії множин, нечітких множин, графів, теорії ігор тощо. Далі синтезуються відповідні алгоритми управління $\{A\}$. В подальшому, на основі створених алгоритмів реалізуються моделі управління $\{M\}$ під можливі варіанти подій в мережі, здійснюється їх координація роботи та інтеграція в системне середовище.

Виконання цілей $\{Z\}$, функцій $\{F\}$, задач управління $\{Z\}$, що були поставлені перед системою управління мережами, повинно гарантувати функціонування ТКМ в цілому, окремих мереж, напрямку, каналу, вузла, маршруту, обладнання з необхідною ефективністю. Система управління мережами досить ефективна, якщо вона забезпечує заданий приріст показника її ефективності. Наявність сукупності критеріїв ефективності обумовлює багатокритеріальність задач управління та значно ускладнює розробку формальних методів:

$$K = \{K_v\}, v = \overline{1, V}.$$

Існує велика кількість методів багатокритеріальної оптимізації [6]. Звичайним рішенням є визначення головного критерій ефективності (виходячи з поточної ситуації в мережі), який підлягає оптимізації, а інші переводити в розряд обмежень. Наприклад, авторами пропонується використати метод ієрархічного цільового динамічного оцінювання альтернатив [8, 9], а саме глобальні (максимальна пропускна здатність, мінімальний час затримки) та локальні (час циклу управління, об'єм службового трафіку) критерії.

Розглянемо декілька критеріїв оцінки ефективності функціонування СУ ТКМ.

Глобальні критерії (оцінюють якість прийнятих рішень системою управління):

1. Максимум (завдане значення) пропускної здатності ρ мережі, яка визначає сумарну пропускну здатність всіх напрямків передачі:

$$\text{мережі } \rho_M = \sum_{i=1}^I \rho_{H_i}.$$

2. Мінімальний час затримки пакетів (завдане значення) t_3 :

$$\min t_3 (t_3 \leq t_{3 \text{ зад}}).$$

Локальні критерії (оцінюють саму систему управління):

1. Мінімальний час циклу управління:

$$T_{\text{ЦУ}} = t_{\text{зі}} + t_{\text{ан}} + t_{\text{пр}} + t_{\text{дов}}, \quad T_{\text{ЦУ}} \leq t_i^{\text{доп}} \rightarrow \min,$$

де $T_{\text{цу}}$ – час циклу оперативного управління мережею – проміжок часу, протягом якого здійснюється послідовне рішення задач управління до повного її виконання в масштабі даної системи управління;

$t_{\text{зі}}$ – час на збір інформації про стан мережі;

$t_{\text{ан}}$ – час на оцінку характеристик мережі та ідентифікацію стану мережі;

$t_{\text{пр}}$ – час, який необхідний на вироблення управлінських рішень;

$t_{\text{дов}}$ – час доведення управлінських впливів до об'єктів управління;

$t_i^{\text{доп}}$ – час, що відведений на оперативне управління мережею, який визначається директивними документами.

2. Мінімальний об'єм службового трафіку $V_{\text{СТ}} \rightarrow \min$ – залежить від прийнятого в СУ мережею способу, об'єму, періоду розсилання службової інформації (маршрутні повідомлення, квитанції, hello-повідомлення, виміри трафіку), складності прийнятих алгоритмів управління, розмірністю мережі, тощо.

3. Фінансово-економічні: вартість розробки та експлуатації системи управління.

Для оцінки ефективності системи управління використовують два типи моделей – аналітичні й імітаційні (статистичні).

За допомогою використання аналітичного або імітаційного моделювання проводиться оцінка ступеня виконання поставлених цілей управління кожного рівня управління та системи управління загалом з урахуванням цілей управління, показників якості функціонування ТКМ, виділеного ресурсу мережі, процесу функціонування ТКМ за відомими алгоритмами.

Найважливішою перевагою аналітичних моделей є те, що результати, отримані на основі їх використання, можуть бути визначені в результаті однократного виконання дій у загальному виді. Останнє дозволяє проводити всебічне дослідження отриманого результату з метою його оптимізації. Однак побудова аналітичної моделі системи зв'язку часто пов'язана із прийняттям ряду допущень, що значно спрощують процес функціонування. Це є наслідком складності адекватного відображення досліджуваного об'єкта.

Імітаційна модель, як правило, не накладає ніяких обмежень на складність модельованої системи й дозволяє враховувати в моделі будь-яке число факторів, що впливають. За певних умов можуть бути використані комбіновані моделі, у яких сполучаються аналітичні й статистичні методи.

Множина функцій та задач управління разом з вихідними даними $\{X, U, E\}$ визначають функціональну модель управління. Авторами пропонується здійснювати цільову координацію функціональних моделей підсистем та інтеграцію рівнів еталонної моделі OSI.

5. Варіанти реалізації (W_δ).

На основі отриманих моделей (M), алгоритмів (A) управління формується множина способів реалізації системи управління, де враховуються технології СУ ТКМ, технічні засоби їх реалізації, апаратне та програмне забезпечення. З урахуванням способів реалізації системи управління, вихідних даних, критеріїв та моделей оцінки ефективності управління формується множина варіантів побудови системи управління (W_δ), яка включає наступні складові: структура системи управління (C); склад системи управління (D); розподіл функцій за рівнями управління (F_l); алгоритми управління підсистемами СУ (A_l); розподіл функцій (задач) по центрам управління ($F_{\text{цу}}$); число посадових осіб на рівнях управління (H_l); технології реалізації системи управління (Технсу); апаратні та програмні засоби (AP), тощо:

$$W_\delta = F(Y(S, U), \Lambda, E, R, Z, C, D, F_l, A_l, F_{\text{цу}}, H_l, \text{Технсу}, AP)$$

де W_δ – δ -й варіант побудови системи управління; Z – цілі управління; R – виділений ресурс; Λ – вхідні потоки даних; E – зовнішні впливи; S – телекомунікаційна мережа; U – управляючий вплив СУ на ТКМ; Y – реалізація вихідного процесу управління; C – структура системи управління; D – склад системи управління; F_l – розподіл функцій за l -м рівнем управління; A_l – алгоритми управління складовими частинами СУ; $F_{\text{цу}}$ – розподіл функцій,

задач по центрам управління; H_l – число посадових осіб на рівнях управління; Технсу – технології реалізації системи управління; AP – вибрані апаратні та програмні засоби; l – рівні управління СУ.

Структура системи управління повинна відповідати тим завданням, які ставляться перед системою управління по управлінню ТКМ. Система управління повинна являти собою ієрархічну організаційно-технологічну систему, що забезпечує змішане (централізоване/децентралізоване) управління телекомунікаційними підсистемами. Управління повинно здійснюватися в реальному масштабі часу.

Організаційно-технічне об'єднання органів автоматизованого управління мережами зв'язку, що входять до складу системи зв'язку (СЗ) ЗСУ, має здійснюватися на основі уніфікації технічних, інформаційних та програмно-апаратних засобів.

Система управління повинна створюватися з орієнтацією на нові інформаційні технології, перспективу зрощування телекомунікаційних і комп'ютерних мереж, методи розподіленої обробки інформації, використання технологій *Internet*, *SDN*, *IP*, а також хмарні технології та інші технології віртуалізації.

В системі управління повинні передбачатися резервні експлуатаційно-технічні засоби для відновлення функціонування основних напрямків зв'язку, а також відновлення управління мережами у зонах відповідальності. Надійність і живучість системи управління повинні бути вище значень цих параметрів ТКМ. Для забезпечення надійності та живучості автоматизованої системи управління зв'язком ЗСУ основні інформаційні та обчислювальні ресурси повинні бути розміщені в географічно рознесених пунктах управління. В перспективі пропонується застосування технологій хмарних середовищ, що будуть реалізовані центрами обробки даних (ЦОД).

Оцінка варіантів побудови системи управління проводиться за наведеними раніше критеріями.

Для отримання оптимального варіанту системи управління мережами краще використовувати метод (векторної) послідовної оптимізації з використанням принципу максимізації суми зважених критеріїв з використанням методів експертних оцінок. Тоді раціональний (оптимальний) варіант системи управління мережами:

$$W^* = \text{opt } W_\delta, \delta = \overline{1, \Omega}.$$

Таким чином, запропонована методологія синтезу сучасної автоматизованої системи управління телекомунікаційними системами військового призначення за п'ятьма етапами. Розглянуто цілі функціонування ТКМ та системи її управління, визначено вимоги до телекомунікаційних підсистем й системи управління та проведено їх детальний опис. Представлений процес функціонування системи управління за етапами та циклами управління. Описано основні функції та задачі управління, які потрібно вирішувати в циклі управління. Визначено перелік моделей й алгоритмів управління, множина функцій, задач управління, які формують функціональну модель управління.

Варіанти побудови системи управління формуються на основі: структури системи управління; складу системи управління; розподілу функцій за рівнями управління; алгоритмів управління за підсистемами СУ; розподілу функцій (задач) по центрам управління; кількості посадових осіб на різних рівнях управління; наявних технологій реалізації системи управління, апаратних та програмних засобів.

Отримані нові наукові результати складають основу методології синтезу систем управління інформаційно-телекомунікаційними мережами. Це дозволить у майбутньому побудувати ефективну систему управління системою зв'язку Збройних Сил України для рішення різного роду завдань планування, розгортання та оперативного управління з використанням технологій інтелектуалізації.

ЛІТЕРАТУРА

1. ДСТУ 3265-1995 Зв'язок військовий. Терміни та визначення.

2. Битнер В. И. Нормирование качества телекоммуникационных услуг: Учебное пособие для вузов / В. И. Битнер, Г. Н. Попов. – М: Горячая линия-Телеком, 2009.
3. Цвиркун А. Д. Основы синтеза структуры сложных систем / А. Д. Цвиркун. – М: Наука, 1982. – 200 с.
4. Design of the Next Generation Military Network Management System Based on NETCONF [Електронний ресурс] / W.Zhu, N. Liu, W. Shan, G. Fu // Information Technology:New Generation. – 2008.
5. Бовда Е. М. Концептуальні основи синтезу автоматизованої системи управління зв'язком військового призначення / Е. М. Бовда, Ю. А. Плугувий, В. А. Романюк. // ВІТІ. – 2016. – №1. – С. 3–17.
6. Хиленко В.В. Методи підвищення показників якості системи управління телекомунікаційними мережами: Монографія / В.В. Хиленко, Л.Н. Беркман, Г.Ф. Колченко, О.Г. Варфоломеева . – К.: Норіта-плюс, 2007.– 236 с.
7. Шибанов В.С. Средства автоматизации управления в системах связи / В.С. Шибанов. – М.: Радио и связь, 1990. – 232 с.
8. Боговик А. В. Эффективность систем военной связи и методы её оценки. / А. В. Боговик, В. В. Игнатов. – СПб: ВАС, 2006.
9. Романюк В.А. Цільові функції оперативного управління тактичними радіомережами /В.А. Романюк// Збірник наукових праць ВІТІ НТУУ "КПІ". – 2012. – № 1. – С. 109 – 117.

д.т.н. Горбенко І. Д. (ХНУ ім. В.Н. Каразіна, АТ „ІТ”)
д.т.н. Потій О.В. (Служба Держспецзв’язку)
к.т.н. Єсіна М. В. (ХНУ ім. В.Н. Каразіна, АТ „ІТ”)
к.т.н. Качко О. Г. (АТ „ІТ”)
д.т.н. Олексійчук А. М. (НТУ „КПІ ім. І. Сікорського”)
д.т.н. Кузнецов О.О. (ХНУ ім. В.Н. Каразіна, АТ „ІТ”)
к.т.н. Горбенко Ю.І. (АТ „ІТ”)

СУТНІСТЬ ПРОБЛЕМ РОЗРОБКИ, СТАНДАРТИЗАЦІЇ ТА ЗАСТОСУВАННЯ ПЕРСПЕКТИВНИХ НАЦІОНАЛЬНИХ СТАНДАРТІВ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ В УКРАЇНІ

Криптографічних захист є безумовно обов’язковою системою надання в процесі обробки інформації в критичних інформаційних інфраструктурах, національній телекомунікаційній мережі, телекомунікаційних системах (мережах), системах спеціального зв’язку та національних системах електронних інформаційних ресурсів, системах електронних комунікацій [1] таких основних криптографічних послуг з безпеки інформації як конфіденційність, цілісність, доступність, неспростовність, захищеність від НСД тощо. Згідно [2] та з урахуванням рішення Європейського Парламенту та Ради ЄС з питань електронної ідентифікації і довірчих послуг [3] повинні надаватись електронні довірчі послуги з електронної ідентифікації, електронної автентифікації, електронного підпису, електронного штамп (печатки), електронної мітки часу, електронного документу, електронної доставки документу та електронної автентифікації веб-сайтів. В ряді випадків особливостями нинішнього етапу розвитку названих систем є використання при їх побудуванні та застосуванні технологій хмарних обчислень, при застосуванні хмарних технологій виникає значне число проблемних питань в частині надання користувачам основних послуг з безпеки інформації на основі застосування криптографічних механізмів. Особливо проблемним є забезпечення КЗІ в критичних інформаційних структурах.

Метою цієї доповіді є аналіз стану та можливостей застосування існуючих криптоперетворень в Україні, визначення шляхів проблем розв’язку проблем побудови та застосування перспективних національних стандартів симетричних та асиметричних криптографічних перетворень та криптографічних протоколів.

1. Стан та проблеми КЗІ в Україні

Основними криптографічними перетвореннями, що застосовуються у залежності від вимог, є симетричні та асиметричні криптографічні перетворення, а також криптографічні протоколи. Їх використання здійснюється засобом шифрування інформації (симетричного та асиметричного), електронного підпису, застосування криптографічних протоколів та управління ключами тощо. Визнано, що вказані криптографічні перетворення повинні бути стійкими проти зламу при застосуванні усіх відомих та потенційно можливих криптоаналітичних атак зі сторони зломисників відповідних рівнів. Основною вимогою до криптографічних перетворень на рівні держави є обов’язковість стандартизації проектів стандартів на національному рівні чи гармонізація та стандартизація міжнародних чи регіональних стандартів і на національному рівні. Наразі є обґрунтовані підозри, що у перехідний та постквантовий період існуючі стандарти криптоперетворень типу симетричний та асиметричний шифр (АСШ), протокол інкапсуляції ключів (ПІК) та електронний підпис (ЕП) [4 – 6] будуть зламуватись за допомогою квантових криптоаналітичних систем криптоаналітиком 3-го рівня з поліноміальною чи суб’експоненційною складністю. Також важливою особливістю постквантового періоду є значна невизначеність щодо вихідних даних для криптоаналізу та протидії в частині можливостей квантових комп’ютерів (КВК), їх математичного та програмного забезпечень, а також застосування для криптоаналізу вказаних асиметричних криптоперетворень. Їх застосування повинне розглядатись щодо перехідного та постквантових періодів. Підтвердженням гостроти вказаних проблем є широкомасштабні дослідження, що ведуться

на міжнародному рівні у вигляді міжнародного проекту NIST США, завданням яких є розробка та стандартизація постквантових криптографічних перетворень типу АСШ, ЕП та ПІК [4, 5]. Що стосується розвитку квантових технологій, то компанія IonQ, розробник апаратного і програмного забезпечення для квантових обчислень, оголосила про відкриття ЦОД для 10 квантових комп'ютерів IonQ [11]. Повідомляється, що новий ЦОД площею 2100 м², розташований на території Університету Меріленда, допоможе компанії в проведенні досліджень і розробці нового обладнання, а самі платформи IonQ будуть доступні для дослідників по всій території США. Частково проект був профінансований за рахунок інвестицій Університету Меріленда в розмірі \$ 5,5 млн.

На наш погляд особливо гострою проблемою щодо політики криптографічного захисту інформації в Україні є використання в якості національних гармонізованих регіональних стандартів, в першу чергу РФ ГОСТ Р 34.11-94 (функція гешування) та ГОСТ 28147-89 (блоковий шифр), а також без належного обґрунтування гармонізація та застосування регіональних та міжнародних стандартів без належного аналізу їх властивостей. Такою ж гострою проблемою є затягування зі впровадженням та використанням національних стандартів ДСТУ 7624:2014, ДСТУ 7564:2014 та ДСТУ 8845:2019 [7 – 9]. Вказані національні стандарти КЗІ щодо їх криптографічної стійкості та ефективності є обґрунтовано постквантовими. Повільно іде підготовка до впровадження постквантового національного стандарту ДСТУ 8961:2019 – Алгоритми асиметричного шифрування та інкапсуляції ключів. Тому, на наш погляд, на рівні держави стоїть проблема обґрунтування, розроблення, дослідження та стандартизації криптографічних систем для постквантового періоду, яка може бути розв'язаною на рівні держави.

2. Стан застосування та розробки систем КЗІ на міжнародному рівні. На міжнародному рівні визнано [4, 5, 7, 8], що у постквантовий період існуючі стандарти асиметричних криптоперетворень, будуть зламуватись за допомогою квантових криптоаналітичних систем криптоаналітиком 3-го рівня з поліноміальною чи суб'експоненційною складністю. Важливою особливістю постквантового періоду є значна невизначеність щодо вихідних даних для криптоаналізу та протидії в частині можливостей квантових комп'ютерів [4-6], їх математичного та програмного забезпечень, а також застосування для криптоаналізу існуючих криптоперетворень та криптопротоколів. NIST США звернув увагу на дану проблемну ситуацію та оголосив конкурс на перспективні постквантові криптографічні примітиви, які наприкінці конкурсу будуть стандартизовані.

Процес стандартизації постквантової криптографії NIST розпочався в 2017 році з 69 алгоритмами-кандидатами, які відповідали як мінімальним критеріям прийняття, так і вимогам подання. Перший раунд тривав до січня 2019 року, протягом якого алгоритми кандидатів оцінювали виходячи з їх безпеки, продуктивності та інших характеристик. NIST вибрав 26 алгоритмів для переходу до другого раунду для подальшого аналізу.

Основні вимоги до кандидатів на стандарти постквантових криптоперетворень можна конкретизувати у трьох таких напрямках [4, 5]: вимоги з безпеки (вимоги щодо стійкості до криптографічного аналізу); техніко-економічні вимоги (в основному щодо часової та просторової складностей); технічні характеристики реалізації алгоритмів асиметричних криптоперетворень. За підсумками 2-го етапу NIST США обрав 26 алгоритмів-кандидатів для 2-го раунду. З 26 кандидатів 17 були механізмами встановлення ключів (КЕМ) або схемами шифрування з відкритим ключем, дев'ять – цифровими підписами (див. табл. 1, 2).

Таблиця 1

Підсумки 2-го етапу конкурсу

Математичний апарат, який використовується	Підпис	КЕМ	Всього
На основі решіток	3	9	12
На основі кодів	0	7	7
На основі багатовимірних перетворень	4	0	4
На симетричній основі	2		2
Інші	0	1	1
Всього	9	17	26

Таблиця 2

Кандидати другого раунду		
Алгоритми KEM		Алгоритми цифрового підпису
BIKE	NTRU Prime	CRYSTALS-DILITHIUM
Classic McEliece	NTS-KEM	FALCON
CRYSTALS-KYBER	ROLLO	GeMSS
FrodoKEM	Round5	LUOV
HQC	RQC	MQDSS
LAC	SABER	Picnic
LEDACrypt	SIKE	qTESLA
NewHope	Three Bears	Rainbow
NTRU		SPHINCS+

При виборі між дуже схожими алгоритмами KEM, вартість і продуктивність були важливими критеріями вибору. При порівнянні кандидатів були враховані як витрати на передачу даних, так і ефективність обчислень [1].

По закінченню 2-го раунду досліджень NIST вибрав 15 кандидатів другого раунду, нині йде третій раунду процесу стандартизації. З 15 висунутих кандидатів сім були обрані в якості фіналістів і вісім в якості альтернативних кандидатів. У таблиці 3 наведено перелік алгоритмів-фіналістів, а у таблиці 4 – перелік альтернативних варіантів алгоритмів.

Таблиця 3

Фіналісти третього раунду	
АСШ/ПІК	ЕП
Classic McEliece	CRYSTALS-DILITHIUM
CRYSTALS-KYBER	FALCON
NTRU	Rainbow
SABER	

Таблиця 4

Альтернативні кандидати	
Асиметричне шифрування/KEM	Цифрові підписи
BIKE	GeMSS
FrodoKEM	Picnic
HQC	SPHINCS+
NTRU Prime	
SIKE	

Набір фіналістів – це алгоритми, які NIST вважає найбільш перспективними для відповідності більшості випадків використання та, швидше за все, які будуть готові до стандартизації незабаром після закінчення третього раунду. У нинішньому представленні NIST схеми на основі алгебраїчної решітки представляються найбільш перспективними універсальними алгоритмами АСШ, ПІК та ЕП [5]. Альтернативні кандидати розглядаються як потенційні кандидати для майбутньої стандартизації, швидше за все, після чергового раунду оцінки. Деякі з альтернативних кандидатів мають гіршу продуктивність, ніж фіналісти, але можуть бути обрані для стандартизації на основі високої впевненості NIST в їх безпеці. Інші мають прийнятну продуктивність, але вимагають додаткового аналізу або іншої роботи, щоб довести свою безпеку для стандартизації NIST. Крім того, деякі альтернативні кандидати були обрані на підставі або прагнення NIST до різноманітності в майбутніх постквантових стандартах безпеки, або їх потенціалу при подальшому покращенні [5].

3. Стан розроблення, стандартизації та застосування симетричних криптоперетворень постквантового періоду в Україні. Наразі розроблені та стандартизовані такі криптоперетворення симетричного типу постквантового періоду:

- Алгоритм блокового симетричного перетворення ДСТУ 7624 :2014 – 10 режимів роботи, (128, 256, 512біт) (5-7 рівня);
- Функція гешування ДСТУ 7564:2014 (8-512 біт) (5-7 рівня);
- Алгоритм симетричного потокового перетворення ДСТУ 8845:2019 (256-512 біт) (5-7 рівень).

3.1 Властивості та параметри ДСТУ 7624:2014 „КАЛИНА-2”

Режим простої заміни є базовим компонентом усіх інших режимів роботи криптографічного алгоритму симетричного блокового перетворення, в тому числі і БСШ „Калина-2”, на якому режими ґрунтуються. Залежність кількості ітерацій (t) при реалізації перетворень $T_{l,k}^{(K)}$ та $U_{l,k}^{(K)}$, кількості стовпців матриці внутрішнього стану (c) від розміру блоку (l) і довжини ключа шифрування (k) наведено у табл. 5. В табл. 6 наведені режими роботи ДСТУ 7624:2014.

Структура перетворення. Базове перетворення зашифрування $T_{l,k}^{(K)}$ визначено у такому вигляді

$$T_{l,k}^{(K)} = \eta_l^{(K_l)} \circ \psi_l \circ \tau_l \circ \pi_l' \circ \left(\prod_{v=1}^{t-1} \left(\kappa_l^{(K_v)} \circ \psi_l \circ \tau_l \circ \pi_l' \right) \right) \circ \eta_l^{(K_0)}. \quad (1)$$

Таблиця 5

Параметри алгоритму СБП „Калина-2”

№ з/п	Розмір блоку (l)	Довжина ключа (k)	Кількість ітерацій перетворення (t)	Кількість стовпців в матриці (c)
1	128	128	10	2
2		256	14	
3	256	256	14	4
4		512	18	
5	512	512	18	8

Таблиця 6

Режими роботи ДСТУ 7624:2014

№ режиму	Назва режиму	Позначення	Послуга безпеки
1	Проста заміна (базове перетворення)	ECB	Конфіденційність
2	Гамування	CTR	Конфіденційність
3	Гамування зі зворотнім зв'язком по шифртексту	CFB	Конфіденційність
4	Вироблення імітовставки	CMAC	Цілісність
5	Зчеплення шифрблоків	CBC	Конфіденційність
6	Гамування зі зворотнім зв'язком по шифр гамі	OFB	Конфіденційність
7	Вибіркове гамування із прискореним виробленням імітовставки	GCM, GMAC	конфіденційність і цілісність (GCM), тільки цілісність (GMAC)
8	Вироблення імітовставки і гамування	CCM	цілісність і конфіденційність
9	Індексованої заміни	XTS	конфіденційність
10	Захисту ключових даних	KW	конфіденційність і цілісність

3.2 Алгоритм симетричного потокового перетворення ДСТУ 8845:2019 (256-512 БІТ) (5-7 рівень)

В основі алгоритму Струмок лежить класична схема підсумовуючого генератора, подібна генератору SNOW-2.0, який визначено в ДСТУ ISO/IEC 18033-4:2015. Алгоритм Струмок використовує 256-бітний вектор ініціалізації IV та 256-бітний або 512-бітний секретний ключ K і забезпечує високий та надвисокий рівень стійкості із врахуванням можливого застосування квантового криптографічного аналізу. Криптоалгоритм орієнтований на 64-розрядні обчислення. Схематичне зображення генератора ключових потоків Струмок у режимі генерації гами шифру (ключового потоку) наведено на рис. 1.

3.3 Функція гешування ДСТУ 7564:2014 (8-512 БІТ) (5-7 рівня)

Алгоритм обчислення геш-значення. Під час формування геш-значення повідомлення M завжди доповнюється до довжини, кратної розміру блоку, та поділяється на блоки $m_1, m_2, \dots, m_k$, кожен з яких має довжину l біт. Вибір l здійснюють відповідно до розміру геш-значення n :

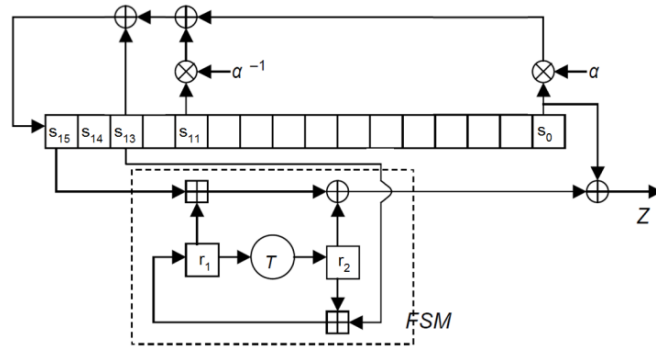


Рис. 1 – Генератор ключових потоків Струмук у режимі генерації гами шифру

$$l = \begin{cases} 512 & \text{для } 8 \leq n \leq 256, \\ 1024 & \text{для } 256 < n \leq 512, \end{cases} \quad (2)$$

де $n \in \{8 \cdot s \mid s = 1, 2, \dots, 64\}$.

Обчислення геш-значення здійснюють за такою ітеративною процедурою:

$$\begin{aligned} h_0 &= IV, \\ h_i &= T_l^\oplus(h_{i-1} \oplus m_i) \oplus T_l^+(m_i) \oplus h_{i-1}, \quad i = 1, 2, \dots, k, \\ H(IV, M) &= R_{l,n}(T_l^\oplus(h_k) \oplus h_k), \end{aligned} \quad (3)$$

$$IV = \begin{cases} 0x4000\dots00 & \text{для } l = 512, \\ 0x8000\dots00 & \text{для } l = 1024 \end{cases} \quad \text{— вектор ініціалізації } l \text{ біт; } T_l^\oplus, T_l^+ \text{ — бієктивні}$$

перетворення, що виконують відображення вхідного блоку довжиною l біт у вихідний такої ж довжини.

Структурна схема функції гешування „Купина” наведена на рис. 2.

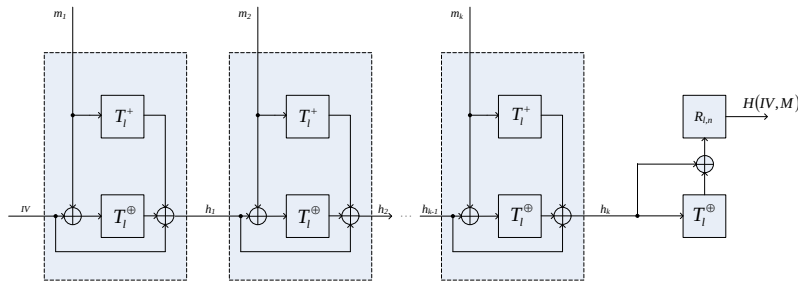


Рис. 2 – Структурна схема функції гешування "Купина"

4. Стан розроблення та стандартизації та застосування асиметричних криптоперетворень постквантового періоду в Україні.

4.1 Стандарт ДСТУ 8961:2019 „СКЕЛІЯ”

Стандарт встановлює криптографічний алгоритм асиметричного шифрування та інкапсуляції ключів для забезпечення конфіденційності, цілісності, доступності, неспростовності та криптоживучості (як додаткової послуги) інформації та ключів під час їх оброблення. У стандарті ДСТУ 8961:2019 описано алгоритми асиметричного шифрування та інкапсуляції ключів, у якому використовуються алгоритми криптографічних перетворень з відкритими ключами.

В алгоритмі асиметричного шифрування використовується асиметрична пара ключів – відкритий ключ для зашифрування блоків інформації (даних) відправником, а особистий (секретний) ключ – для розшифрування зашифрованих блоків отримувачем.

В алгоритмі (протоколі) інкапсуляції ключів також використовується асиметрична пара ключів – особистий (секретний) ключ сеансу – для інкапсуляції ключа сеансу відправником, а відкритий ключ сеансу – для декапсуляції сеансового ключа отримувачем.

Отримувач на основі свого секретного (особистого) ключа розшифрування та декапсулюваного ключа сеансу відправника, а відправник на основі відкритого ключа зашифрування отримувача та свого секретного ключа сеансу, виробляють спільну таємницю (спільний ключ). В подальшому спільний ключ може використовуватись для шифрування інформації (даних) в каналах зв'язку при обміні інформацією. Інкапсуляція ключа представляє процес криптографічного перетворення ключа сеансу та інших даних з метою забезпечення їх конфіденційності, цілісності (справжності) та криптоживучості, а також узгодження ключа симетричного шифрування даних між відправником та отримувачем в подальшому. Декапсуляція представляє собою процес перевірки цілісності та справжності інкапсульованого ключа сеансу зв'язку та узгодження ключа захисту даних між отримувачем та відправником.

Шифрування та інкапсуляція ключів здійснюється на основі математичних перетворень в кільці поліномі над скінченим полем. При розробленні стандарту враховані вимоги щодо забезпечення криптографічної стійкості проти спеціальних атак на основі витoku по технічних каналах, а також потенційних класичних та квантових атак, в тому числі у перехідний та постквантовий періоди. Стандарт розроблено з урахуванням досвіду створення та застосування стандартів ДСТУ ISO/IEC 18033-2:2015, ANSI X9.98-2010. Цей стандарт може використовуватись під час розробки систем, комплексів та засобів криптографічного захисту інформації при наданні користувачам послуг конфіденційності, цілісності, неспростовності, доступності та криптоживучості ключів, що узгоджуються відправником та отримувачем, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, в тому числі для захисту від спеціальних атак, а також у перехідний та постквантовий періоди.

Стандарт орієнтований на використання таких національних стандартів (не обов'язково): ДСТУ 7564-2014, ДСТУ 7624-2014, ДСТУ ISO/IEC 18033-2:2015.

Стандарт, у залежності від рівня криптографічної стійкості проти класичних та квантових атак, яку необхідно забезпечити, може застосовуватись в трьох режимах роботи:

- режим Склея – КЕМ 256/128 – 256 біт захисту від класичних атак та 128 біт захисту від квантових атак, а також захисту від спеціальних атак;
- режим Склея – КЕМ 384/192 – 384 біт захисту від класичних атак та 192 біт захисту від квантових атак, а також захисту від спеціальних атак;
- режим Склея – КЕМ 512/256 – 512 біт захисту від класичних атак та 256 біт захисту від квантових атак, а також захисту від спеціальних атак.

Також в кожному із режимів роботи можуть використовуватись окремо такі криптографічні перетворення:

- незалежний алгоритм (функція) асиметричного шифрування;
- протокол інкапсуляції ключів (функція), що ґрунтується на використанні функції асиметричного шифру;
- механізм (функція) симетричного шифрування та автентифікації, що ґрунтується на функціях асиметричного шифрування та інкапсуляція ключів.

В кожному із режимів роботи за рахунок застосування криптографічних перетворень в кільцях поліномів та скінчених полях забезпечується надання послуг конфіденційності, цілісності, справжності, доступності та криптографічної живучості ключа сеансу зв'язку та його узгодження між відправником та отримувачем.

ВИСНОВКИ

1. В процесі створення системи КЗІ гарантувати державним відомствам, органам та користувачам надання електронних довірчих послуг згідно вимог законів «Про електронні довірчі послуги» та «Про основні засади забезпечення кібербезпеки України».

2. Необхідно удосконалити нормативно-правову базу у сфері КЗІ у відповідності з існуючими визнаними на міжнародному рівні регламентами, стандартами та підходами і положеннями.

3. В міру можливостей оперативно, вивести із дії регіональні стандарти КЗІ РФ (ДСТУ ГОСТ 34.311-2009, ДСТУ ГОСТ 28147-2009), щодо яких маються підозри щодо їх стійкості та безпечності застосування, а також їх низької продуктивності.

4. Оперативно ввести в дію національні стандарти КЗІ – ДСТУ 7564-2014, ДСТУ 7624-2014, ДСТУ 8845:2019 та ДСТУ 8961:2019 та їх нормативно-правове забезпечення тощо.

5. Розробити та прийняти у якості національних комплекс стандартизованих асиметричних та симетричних криптоперетворень, при використанні яких будуть забезпечені вимоги до них як в перехідний, так і постквантовий періоди.

6. Теоретично обґрунтувати та ввести у дію комплексні моделі порушників, моделі загроз та криптографічної безпеки щодо симетричних та асиметричних криптопримітивів, в тому числі для їх застосування в перехідний та постквантовий періоди.

7. Обґрунтувати та законодавче оформити вимоги до перспективних криптографічних примітивів, систем та засобів КЗІ.

ЛІТЕРАТУРА

1. Закон України «Про основні засади забезпечення кібербезпеки України». – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.

2. Закон України «Про електронні довірчі послуги». – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>.

3. РЕГЛАМЕНТ (ЄС) № 910/2014 ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ ТА РАДИ від 23 липня 2014 року «Про електронну ідентифікацію та довірчі послуги для електронних транзакцій в межах внутрішнього ринку та про скасування Директиви 1999/93/ЄС» (1)(COM (2012) 0238 – C7-0133/2012 – 2012 / 0146 (COD)).

4. Post-Quantum Cryptography. Round 2 Submissions. [Електронний ресурс] – Режим доступу: <https://csrc.nist.gov/Projects/post-quantum-cryptography/round-2-submissions>.

5. Gorjan Alagic Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8309 / Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone // 22 July 2020. – Режим доступу: <https://doi.org/10.6028/NIST.IR.8309>.

6. Горбенко Ю. І. Методи побудування та аналізу криптографічних систем: / Ю. І. Горбенко. Х.: Форт, 2015. – 959 с.

7. ДСТУ 7624:2014 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Мінекономрозвитку України, 2016. – 228 с.

8. ДСТУ 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функція гешування. – Мінекономрозвитку України, 2015. – 39 с.

9. ДСТУ 8845:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=82494.

10. ДСТУ 8961:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=88056.

11. IonQ відкрила перший квантовий дата-центр. [Електронний ресурс] – Режим доступу: <https://portaltele.com.ua/news/companies/ionq-vidkryla-pershyj-kvantovyj-data-tsentr.html>.

НАПРЯМКИ ВДОСКОНАЛЕННЯ РЕЖИМУ ППРЧ У ВІЙСЬКОВИХ ЗАСОБАХ РАДІОЗВ'ЯЗКУ

Сучасні військові радіозасоби функціонують в умовах складної електромагнітної обстановки. Забезпечення надійного радіозв'язку в умовах впливу навмисних і ненавмисних завад можливе при використанні сигналів з розширеним спектром.

Основними методами розширення спектра сигналів є безпосередня модуляція несучої псевдовипадкової послідовності (пряме розширення спектра) та псевдовипадкова перебудова робочої частоти (ППРЧ) [1].

У сучасних радіозасобах військового призначення, що знаходяться на озброєнні у провідних країнах, а саме „Harris” (США), „Thales” (Франція), „Aselsan” (Туреччина), „Elbit” (Ізраїль), комплексів „Акведук”, „Азарг”, „Граніт” (Російська Федерація) та ін. широко використовується режим ППРЧ [2], принцип роботи якого полягає у тому, що радіостанції кореспондентів синхронно та швидко (декілька сотень і більше стрибків за секунду) за невідомим постановнику завад псевдовипадковим законом переходять на нову радіочастоту. При цьому задача радіоелектронного подавлення радіомереж значно ускладнюється.

Успішність функціонування радіомереж з ППРЧ значною мірою залежить від технічних можливостей засобів радіоелектронної боротьби (РЕБ) противника, а також швидкості перебудови частоти, кількості номіналів частот, на які можуть переходити засоби радіозв'язку (ЗРЗ), ширини смуги, у межах якої здійснюється перебудова робочої частоти (так званого хопсета), рівня адаптації до стану радіоканалу, автоматизації та інтелектуалізації системи управління радіомережею в цілому та окремими радіозасобами зокрема [2]. Так, для ефективного подавлення постановник завад (ПЗ) повинен розподілити енергію станції завад (СЗ) у всій смузі роботи радіомережі з ППРЧ (шумова загороджувальна завада), або перекрити певну ділянку цієї смуги (шумова завада у частині смуги). При цьому енергії передавача СЗ може виявитися недостатньо. Іншими (більш енергетично ефективними) варіантами подавлення є застосування завад у відповідь, полігармонійних (багатотональних) або комбінованих завад [1]. Метою постановника завад є постановка такої завади, яка при загальній обмеженості потужності передавача станції завад P_z повинна забезпечити мінімізацію відношення сигнал/завада на виході приймача ЗРЗ.

Поряд з беззаперечними перевагами, ЗРЗ з ППРЧ притаманні й певні недоліки [2]:

за певних умов станції завад здатні подавлювати системи з ППРЧ;

підвищені вимоги до системи синхронізації;

створення взаємних завад військовим та цивільним радіозасобам, смуги робочих частот яких потрапляють у смуги систем з ППРЧ, або частково перекриваються;

зниження швидкості передачі даних та дальності зв'язку у порівнянні з системами на фіксованих частотах.

Тому метою доповіді є визначення напрямків удосконалення засобів радіозв'язку з ППРЧ.

Підвищення стійкості до впливу навмисних завад противника. Розв'язання задач, спрямованих на підвищення завадозахищеності ЗРЗ з ППРЧ може бути реалізовано у рамках технології програмованих радіостанцій – SDR та радіостанцій з інтелектуальним управлінням [4]. Підхід до побудови інтелектуальних радіосистем отримав назву когнітивного радіо. Основи технології когнітивних радіосистем представлені, зокрема, у вигляді стандарту IEEE 802.22. Когнітивна радіосистема може отримувати знання про середовище експлуатації та свій внутрішній стан, на основі чого динамічно та автономно коригувати власні експлуатаційні параметри та протоколи для досягнення поставлених раніше цілей і навчатися на основі отриманих результатів [5].

Загальними заходами підвищення завадозахищеності (незалежно від стратегії постановника завад) у радіозасобах як з ППРЧ, так і на фіксованих частотах, є наступні [6]:

просторова фільтрація завад, використання направлених антен, адаптивних антенних решіток;

зменшення відстані між ЗРЗ, що забезпечить зростання відношення сигнал/завада (BCЗ) на входах приймачів. Це може бути забезпечено у мобільних радіомережах класу MANET за рахунок можливості забезпечення ретрансляцій кожною радіостанцією.

Відомо, що існує деяка оптимальна стратегія постановника *шумових завад* (загороджувальної та у частині смуги), яка полягає у концентрації потужності у певній ділянці хопсета, що забезпечує мінімізацію відношення сигнал/завада (BCЗ) на вході приймачів ЗРЗ [1 – 3]. Тому підвищення завадозахищеності при забезпеченні заданих швидкостей передачі та дальності зв'язку при впливі шумових завад можна досягнути наступними заходами [2]:

зміна ширини хопсета, його центральної частоти;

збільшення потужності передавача;

відключення частот (припинення передачі корисної інформації), перекритих завадою.

У сучасних ЗРЗ з ППРЧ розширення хопсета можливо реалізувати двома шляхами. Перший дозволяє змінювати відповідні налаштування на радіостанції, а другий полягає у створенні запасних каналів з хопсетами в інших ділянках робочого діапазону частот, та/або з хопсетами з більшою шириною. В обох випадках успішність функціонування радіомережі визначатиметься організаційними заходами, які визначають порядок входження в зв'язок у випадку впливу засобів РЕБ, та досвідом операторів (користувачів). Слід зауважити, що зі збільшенням ширини хопсета погіршується якість зв'язку, а отже – зменшується дальність зв'язку. Якщо дальність необхідно зберегти на тому ж рівні – слід зменшувати швидкість передачі інформації. Тому напрямком удосконалення радіозасобів при впливі шумових завад є розробка методик вибору параметрів радіостанцій, які дозволять без участі оператора забезпечувати автоматичний вибір необхідної середньої частоти та ширини хопсета, потужності передавача, кількості активних (невідключених) частот у хопсеті для забезпечення заданої швидкості, якості та дальності зв'язку. Першочерговим завданням при цьому є реалізація процедур оцінки стану каналу, ідентифікації типу завад, поточних значень їх параметрів та стратегії постановника завад в цілому.

Задача практичної реалізації таких методик ускладнюється необхідністю забезпечення зворотного зв'язку (зміна параметрів повинна виконуватися синхронно усіма радіостанціями у визначений момент часу за командою з однієї з станцій, яка повинна координувати функції управління підсистемою завадозахисту радіомережі).

Сучасні радіостанції з ППРЧ переважно використовують обмежену кількість частот, незважаючи на ширину хопсета, що значно спрощує завдання постановника завад. Наприклад, радіостанції Р-002 (Р-005, Р-030) виробництва ТОВ „Телекарт-Прилад”, МСТР-7200НН („Elbit Systems”) можуть використовувати до 256 частот, радіостанції VRC-9661 („Aselsan”) – до 500. Для ускладнення завдання постановнику *полігармонійних* (багатотональних) завад, або комбінованих завад, що складаються з полігармонійних та шумових у частині смуги, кількість частот у хопсеті повинна бути якомога більшою, крім цього доцільно передбачити зміну (адаптивну або за певним законом) їх номіналів.

З погляду енергетичних можливостей найбільш ефективними для подавлення ЗРЗ з ППРЧ є *завади у відповідь*. Їх ефективність не залежить від коефіцієнта виграшу, який має ЗРЗ за рахунок розширення спектру сигналів [1]. Проте створення завад у відповідь за порівняно короткий час передачі частотних елементів сигналу (стрибків частоти) нашоветується на технічні і організаційні труднощі.

Складність, з якою стикаються при постановці завад у відповідь, полягає в обмеженні за часом передачі завади, а також обмеженні передавачів станцій РЕБ по потужності. При перехопленні одночасно декількох сигналів в різних частотних каналах, СЗ необхідно розподілити свою потужність, щоб подавити виявлені сигнали, або відокремити сигнал тієї

СРЗ, що потрібно подавати. При виборі швидкості ППРЧ у військових УКХ радіостанціях необхідно враховувати, що зі збільшенням швидкості ППРЧ підвищується захищеність від організованих завад і погіршуються умови для виявлення і пеленгації, але у той же час, підвищується вартість радіостанцій, погіршується електромагнітна сумісність, зростає час синхронізації, зменшується дальність зв'язку та швидкість передачі даних. Вважається, що на даний час прийнятні швидкості ППРЧ лежать у діапазоні 50-600 стр/с [3].

На рис. 1 показано обвідну і часові інтервали окремих складових частотного елемента при міжсимвольній ППРЧ [3]. На рисунку прийнято наступні позначення: T_{zi} – інтервал часу, протягом якого синтезатор частоти не видає напруги („мертвий” час); $T_{пн1}$, $T_{пн2}$ – інтервали часу наростання і спаду фронтів частотного елемента, відповідно; $T_{акт}$ – інтервал часу, протягом якого частотний елемент має повну амплітуду і передаються інформаційні та кодові символи („активний” час); час $T_{пер} = T_{пн1} + T_{пн2} + T_{zi}$ називається інтервалом переключення. З урахуванням введених позначень тривалість стрибка частоти $T_{заг} = T_{акт} + T_{пер}$.

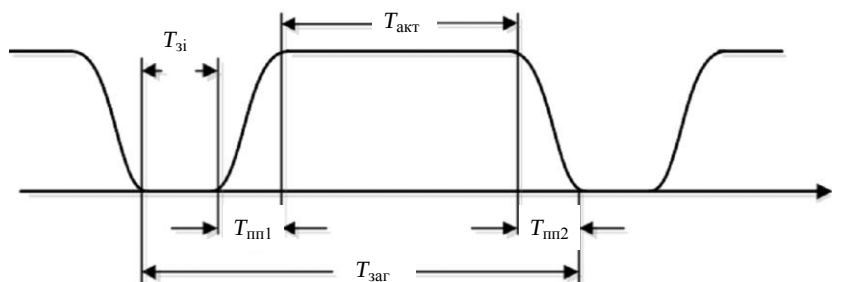


Рис. 1. Обвідна і часові інтервали окремих складових частотного елемента сигналу ППРЧ

Очевидно, що чим більша швидкість перебудови частоти, тим меншою буде інформаційна швидкість, оскільки час переключення $T_{пер}$ не можна довільно зменшувати з ряду причин: обмежена швидкодія синтезатора частоти збуджувача передавача; „дзвін” на виході фільтра проміжної частоти приймача; підсилення завад від сусідніх частотних каналів приймача та ін. Це підтверджується й аналізом характеристик радіостанцій з ППРЧ. У табл. 1 систематизовано дані по швидкості передачі даних для радіостанції Harris RF-7850M-НН [2].

Таблиця 1

Швидкість ППРЧ	Передача голосу (ширина каналу 25 кГц)	Передача даних (ширина каналу 75 кГц)	Передача даних (ширина каналу 25 кГц)
Фіксована частота	16 кбіт/с (CVSD), 2,4 кбіт/с (MELP)	192 кбіт/с	64 кбіт/с
100	16 кбіт/с (CVSD), 2,4 кбіт/с (MELP)	64 кбіт/с	16 кбіт/с
300	12 кбіт/с (CVSD), 2,4 кбіт/с (MELP)	48 кбіт/с	-
1000	Тільки 2,4 кбіт/с MELP	-	-

У радіостанціях комплексу „Азарт” (РФ) швидкість ППРЧ досягає до 20000 стр/с, при цьому швидкість передачі даних складає всього 7,2 кбіт/с [3]. Зменшення інформаційної швидкості при зростанні швидкості ППРЧ пов'язане з тим, що час переключення залишається незмінним, а активний час частотного елемента зменшується, тому відношення $T_{акт}/T_{заг}$ зменшується при $T_{пер} = \text{const}$. В існуючих радіостанціях пауза між випромінюванням на сусідніх частотних елементах ($T_{пер}$) складає близько 10 % від часу однократного використання частоти $T_{заг}$ [3]. Якщо передача мови не потребує високих швидкостей

передачі, то при передачі даних виникає завдання досягнення максимально можливої швидкості, а отже і зменшення швидкості перестройки частоти.

В умовах впливу завад у відповідь виникає декілька задач, які повинні бути реалізовані у відповідних алгоритмах (режимах) роботи радіостанцій:

1) забезпечення мінімально необхідної швидкості ППРЧ при якій коефіцієнт перекриття завадою частотного елемента дорівнює нулю (або близький до нуля), а швидкість передачі даних – максимально можлива (при забезпеченні ймовірності бітової помилки не більше 10^{-6} [7]);

2) на етапі входження в зв'язок необхідно забезпечити максимальну дальність зв'язку (для визначення найбільш віддалених кореспондентів) при мінімально необхідній швидкості передачі інформації;

3) для забезпечення максимальної прихованості передачі інформації та розвідзахищеності, необхідно забезпечити максимізацію швидкості ППРЧ та мінімізацію потужності передавача при заданих швидкості передачі інформації та дальності. При передачі мови швидкість фіксована, тому оптимізація параметрів може зводитися або до забезпечення необхідної дальності зв'язку (мінімізація швидкості ППРЧ), або до підвищення завадозахищеності (максимізація швидкості ППРЧ). При цьому ймовірність бітової помилки повинна складати $10^{-2} \dots 10^{-3}$ [7];

4) збільшення ширини хопсета, а також кількості частот у ньому, призведе до зростання часу виявлення нової робочої частоти приймачем станції радіотехнічної розвідки, тому їх слід збільшувати при значному коефіцієнті перекриття завадою частотних елементів сигналу.

Крім цього, підвищення завадозахищеності при передачі мови (відео) може бути досягнуто застосуванням алгоритмів перемежування потоку даних на виході аналого-цифрового перетворювача [8]. Параметрами, значення яких можуть змінюватись при забезпеченні як передачі даних, так і мови, є швидкість перебудови частоти, швидкість передачі (при передачі даних), ширина хопсета, потужність передавача.

Забезпечення спільної роботи багатьох радіомереж у загальній смузі частот. У систему зв'язку з ППРЧ спочатку закладений елемент „ненадійності”. Це викликано тим, що одночасно на одних частотах працює кілька незалежних систем зв'язку, що призводить до випадкових збігів частот, тобто до виникнення внутрішньосистемних завад, що знижують значення коефіцієнта готовності зв'язку.

В СРЗ з ППРЧ ймовірність взаємних завад можна зменшити шляхом збільшення кількості частотних каналів (розширення хопсета). Крім цього, важливо обирати вид модуляції з якомога компактнішим спектром, наприклад, частотна маніпуляція без розриву фази [9]. Організаційним заходом, спрямованим на зниження внутрішньосистемних завад є урахування частот інших радіоелектронних засобів (РЕЗ) при плануванні хопсетів, введення у радіостанції заборонених смуг частот (це дозволить забезпечити електромагнітну сумісність (ЕМС) з іншими РЕЗ при налаштуванні радіозасобів з ППРЧ, оскільки в більшості з них є можливість виключити потрапляння робочої частоти у певні смуги частот). Зокрема, при налаштуванні радіозасобів виробництва „Aselsan” передбачається процедура частотної оптимізації, яка дозволяє створювати декілька радіомереж у одній спільній смузі частот шляхом призначення різних частот різним радіомережам. При цьому, для радіозасобів різних радіомереж, які знаходяться поряд (у одному транспортному засобі) призначення частот у хопсети відбувається з урахуванням потенційного впливу небажаних гармонік.

Забезпечити узгоджене спільне використання частот різними радіомережами з мінімально допустимим рівнем взаємних завад можна за рахунок псевдовипадкових послідовностей (ПВП), за законами яких змінюються робочі частоти радіомереж, що працюють поряд [10, 11] (шляхом забезпечення мінімально можливих значень взаємкореляційної функції). Крім цього, необхідно врахувати, що від криптографічної стійкості ПВП залежить стійкість СРЗ від розкриття радіотехнічною розвідкою закону перестройки частоти.

Система синхронізації. Прийом і обробка сигналів ППРЧ вимагає точної синхронізації між опорними ПВП приймача і передавача.

Тільки в разі, коли параметри сигналу, в тому числі і його запізнювання за часом, відомі в точці прийому, можлива ефективна робота приймального пристрою СРЗ. В реальних умовах з цілого ряду причин (нестабільність генераторів в передавачі і приймачі, затримка сигналу при поширенні від передавача до приймача і ін.) точний момент приходу сигналу на вхід приймача невідомий.

Система синхронізації в режимі ППРЧ виконує наступні завдання:

первинна синхронізація всіх радіостанцій СРЗ;

поточна синхронізація радіостанцій в процесі обміну інформацією;

введення в будь-який час в синхронізм з радіомережею радіостанції, яка з яких-небудь причин вийшла з синхронізму;

введення в синхронну радіомережу нових радіостанцій.

Виходячи з цих завдань, до системи синхронізації висуваються наступні вимоги [12]:

процес синхронізації повинен бути автоматичним і займати мінімальний час;

синхронізація повинна забезпечуватися при гранично низьких значеннях сигналу на вході приймача;

синхронізація повинна зберігатися протягом тривалих проміжків часу за рахунок місцевих джерел синхронізації (при неприйнятті окремих або декількох кодограм синхронізації, в режимі радіомовчання і т.д.);

кодограми синхронізації повинні бути захищені від навмисних, випадкових завад;

кодограми синхронізації (за формою, положенням в інформаційному потоці) повинні бути невиразні для радіорозвідки противника;

система синхронізації не повинна вимагати „мітки” істинного часу перед входженням в синхронізм.

Завадозахищеність радіолінії (радіомережі) з ППРЧ, в першу чергу, залежить від завадозахищеності алгоритму входження в синхронізм. Тому задача визначення оптимальних значень характеристик алгоритмів входження в синхронізм радіолінії з ППРЧ за критерієм максимальної завадозахищеності є актуальною, важливою і потребує вирішення. На основі аналізу відомих алгоритмів входження в синхронізм можна зробити висновок про те, що шляхом вибору значень характеристик алгоритму можливо досягти якої завгодно високої завадозахищеності в обмін на час входження [12]. Проте необхідно забезпечити баланс між завадозахищеністю синхронізації і якістю передачі корисної інформації при наявності завад. Тобто, рівень завадозахищеності синхронізації треба задавати, виходячи з можливості передачі інформації з необхідною якістю та швидкістю у каналі з завадами, а потім мінімізувати час синхронізації.

У сучасних ЗРЗ з ППРЧ забезпечення синхронізації спрощується за рахунок використання прийому сигналів GPS. Проте, слід враховувати можливий вплив завад на канали прийому GPS, можливе перебування радіостанцій поза зоною покриття супутників. Тому система синхронізації повинна ефективно підтримувати синхронізм як за допомогою прийнятих сигналів GPS, так і з використанням власного високостабільного опорного кварцового генератора [13].

Застосування перспективних методів кодування при формуванні та обробці сигналу з ППРЧ. Відносно новим є метод, який використовує розширення спектру сигналу корельованими стрибками по частоті – CHESS (Correlated Hopping Enhanced Spread Spectrum) [4, 14, 15]. При його реалізації дані кодуються за допомогою методики диференціальної стрибкоподібної перебудови частоти (DFH) – номінал наступного частотного елемента (частотного стрибка) F_N визначається значеннями попереднього частотного елемента (ЧЕ) F_{N-1} та символом даних, що передається X_N :

$$F_N = G(F_{N-1}, X_N),$$

де функція G може розглядатися як направлений граф, вершини якого пов'язані з кодовими комбінаціями даних, що передаються, а ребра відповідають можливим наступним значенням частот. Кількість вершин графа визначається з виразу:

$$v = 2^k,$$

де k – довжина кодової комбінації (кількість бітів, що передається на одному частотному елементі).

Очевидно, що після передачі певної кодової комбінації існуватиме певна кількість дозволених частот, які можуть бути отримані після надходження наступної кодової комбінації, інші значення частот будуть забороненими (неможливими) на даному частотному елементі. Завдяки цьому така система має можливість виправляти помилки (відновлювати втрачену інформацію на неприйнятих (зашумлених) частотних елементах) за рахунок декодування за схемою Вітербі [16]. У той же час, при реалізації CHESSE ускладнюється схема побудови приймача, який, по суті, перетворюється на багатоканальний приймач сигналу багатопозиційної частотної маніпуляції. Перспективним напрямком є реалізація кодування частот за схемою згорткового кодера, що додатково підвищить коригувальну здатність при деякому зменшенні інформаційної швидкості передачі. На рис. 2 наведено приклад несистематичного згорткового кодера зі швидкістю кодування $2/3$. У цьому випадку кількість частот у системі при заданому значенні довжини кодової комбінації зменшується. Наприклад, на рис. 2 для $k = 2$ необхідно 8 частот, у той час як при класичному методі CHESSE – 16 (з кожної вершини графа буде виходити 4 ребра).

Діаграма станів кодера подана на рис. 2, б. Різні стани кодера (вершини графа) позначені літерами a, b, c, e , кожній з яких відповідає двозначна кодова комбінація.

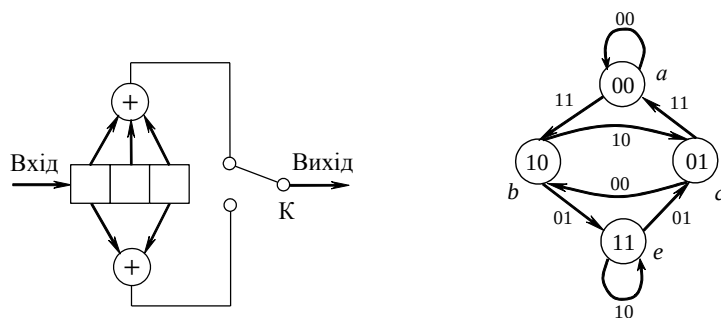


Рис. 2. Несистематичний згортковий код:
а) – структурна схема кодера ; б) – діаграма станів (направлений граф)

Між процедурою кодування згортковим кодом і решіткою мається взаємно однозначна відповідність, яка задається такими правилами [16]:

кожна вершина (вузол) відповідає внутрішньому стану кодера;

ребро, яке виходить з кожної вершини, відповідає одному з можливих символів джерела (для двійкового джерела з кожної вершини виходить два ребра – верхнє для 0 і нижнє для 1). Крім цього, кожне ребро на графі у даному випадку відповідає своїй частоті;

над кожним ребром відзначені значення символів, переданих у канал зв'язку, якщо кодер знаходився в стані, який відповідає даній вершині, і джерело видало символ, що відповідає даному ребру;

послідовність ребер (шлях на решітці) – це послідовність символів, виданих джерелом, та, відповідно, послідовність зміни робочої частоти.

Визначена послідовність початкових інформаційних символів задає конкретну послідовність зміни станів і при цьому виробляє кодові символи на виході кодера (по суті задає нову робочу частоту).

Комбінації вихідних символів записані над ребрами діаграми, стрілки яких показують можливі переходи між станами.

При розгортанні діаграми станів за часом можна одержати решітчасту діаграму, зображену на рис. 3.

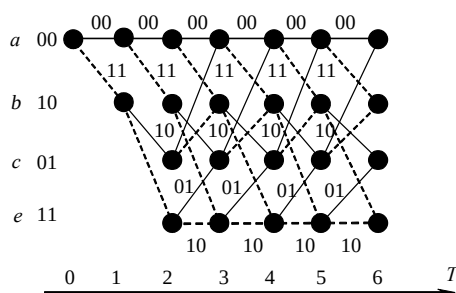


Рис. 3. Решітчаста діаграма згортного коду

На діаграмі показаний перехід по гілці суцільною лінією, якщо початковий інформаційний символ 0 і пунктирною, якщо початковий інформаційний символ 1.

Решітчаста діаграма дає наочне представлення всіх дозволених (можливих) шляхів, якими може просуватися кодер при кодуванні (всіх дозволених змін робочої частоти).

Метод розширення спектра CHESH в різних умовах демонструє кращі або аналогічні показники за енергетичною ефективністю, прихованістю, розвід- та завадозахищеністю в умовах впливу різних типів навмисних завад, а також складністю практичної реалізації у порівнянні з класичною системою ППРЧ та системами з прямим розширенням спектра [4, 14]. Крім цього, CHESH володіє такими перевагами:

- спрощення реалізації множинного доступу до каналу (MAC);

- здатність відновлювати втрачені частотні елементи, виправляти помилки, які виникають за рахунок помилкових спрацьовувань;

- спрощені вимоги до системи синхронізації (можливість самосинхронізації).

Метод CHESH було розроблено для підвищення швидкості передачі даних у короткохвильових радіомережах з ППРЧ [14]. У той же час його застосування може стати перспективним напрямком підвищення ефективності радіомереж і в УКХ діапазоні.

Подальшим розвитком технології CHESH стала HODFH (High Order Differential Frequency Hopping) [15]. На відміну від традиційної DFH, де інформація кодується різницею частот між сусідніми стрибками з, ідея HODFH полягає у використанні кодування за допомогою різних значень частоти і фази (подібно до багатопозиційної модуляції).

Висновки. Таким чином, для забезпечення передачі інформації в умовах активної радіоелектронної протидії противника у сучасних військових засобах радіозв'язку використовується режим ППРЧ.

Основним недоліком існуючих ЗРЗ з ППРЧ є відсутність автоматичної адаптації до стану каналу зв'язку – швидкість перестройки частоти, ширину смуги частот, швидкість передачі інформації, потужність та інші параметри повинні змінювати оператор радіостанції.

Тому перспективними напрямками подальших досліджень є наступні:

- розробка методик, які забезпечать автоматичний вибір параметрів засобів радіозв'язку з ППРЧ в залежності від поточної сигнально-завадової обстановки у каналі зв'язку;

- удосконалення методів оцінки каналу для ідентифікації параметрів завад;

- інтелектуалізація процесів ведення радіозв'язку шляхом впровадження технології SDR та створення когнітивних радіостанцій;

- пошук оптимальних алгоритмів входження в синхронізм радіоліній з ППРЧ;

- побудова систем радіозв'язку на основі технологій розширеного спектру з використанням ефективних сигнально-кодових конструкцій.

ЛІТЕРАТУРА

- Борисов В.И., Зинчук В.М., Лимарев А.Е. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты. Под ред. В.И. Борисова; изд. 2-е, перераб. и доп. М.: Радио Софт, 2008. 512 с.

2. Напрямки вдосконалення засобів радіозв'язку з псевдовипадковою перестройкою робочої частоти / Гурський Т.Г., Жук О.Г., Кривенко О.В., Шишацький А.В. Збірник наукових праць ВІТІ. 2016. № 1. С. 25 – 34.
3. Макаренко С. И., Иванов М. С., Попов С. А. Помехозащищенность систем связи с псевдослучайной перестройкой рабочей частоты. Монография. СПб.: Свое издательство, 2013. 166 с.: ил.
4. Перспективы построения сетей радиосвязи на основе программно-определяемых радиосредств в интересах специальных потребителей / Бондаренко Л.А., Масесов Н.А., Малых В.В., Андреев К.В. Сучасні інформаційні технології у сфері безпеки та оборони. Науковий журнал. 2015. №1 (22). С. 29 – 33.
5. Рекомендации по внедрению стандарта беспроводной связи IEEE 802.22 в системах радиосвязи специального назначения / Масесов Н.А., Панченко И.В., Бондаренко Л.А., Малых В.В. Збірник наукових праць ВІТІ НТУУ „КПІ”. 2013. № 1. С. 24 – 30.
6. Гурський Т.Г. Напрямки підвищення завадозахищеності військових радіомереж класу MANET. Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв'язку та автоматизації в операції Об'єднаних сил: зб. тез доп. XI наук.-практ. конф. ВІТІ. Київ: ВІТІ, 2018. С. 13–19.
7. Investigating communication architecture for tactical radio networks design / B. Suman, S.C. Sharma, M. Pant, S. Kumar. International Journal of Research in Engineering & Applied Sciences. 2012. Vol. 2, Issue 2. Pp. 106 – 118.
8. Гурський Т.Г., Кривенко О.В. Методика формування сигналу в радіозасобах з ППРЧ при передачі мови в умовах впливу завад у відповідь. Системи управління, навігації та зв'язку. 2017. Випуск 2 (42). С. 179 – 184.
9. S. Talarico, M. C. Valenti, D. Torrieri. Optimization of an Adaptive Frequency-Hopping Network. IEEE Military Commun. Conf. (MILCOM). 2015. URL: <http://arxiv.org/pdf/1508.05694.pdf>.
10. M. C. Valenti, D. Torrieri, S. Talarico. Adjacent-channel interference in frequency-hopping ad hoc networks. In Proc. IEEE Int. Conf. on Commun. (ICC), (Budapest, Hungary). Jun. 2013. URL: <https://arxiv.org/pdf/1303.0567.pdf>.
11. Т.Г. Гурський, О.Г. Жук, С.О. Клімович. Напрямки застосування псевдовипадкових послідовностей в радіомережах спеціального призначення. Вісник Хмельницького національного університету. Технічні науки. 2012. № 6. С. 160 – 167.
12. А.С. Коломиец, А.С. Жученко, А.П. Барда. Синхронизация в системах радиосвязи с псевдослучайной перестройкой рабочей частоты. Радиоэлектронні і комп'ютерні системи. 2006. № 2 (14). С. 10 – 14.
13. On accurate time synchronization of multi-sensor mapping systems / C. Toth, S.W. Shin, D. A. Grejner-Brzezinska, J. Hyoun Kwon. Journal of Applied Geodesy. 2008. № 2. – Pp. 159 – 166.
14. AFRL-IF-RS-TR-2001-159 Final Technical Report August 2001, Correlated hopping enhanced spread spectrum (chess) study. URL: <https://apps.dtic.mil/sti/citations/ADA394991>.
15. Y. Li, F. Yao, and B. Xu. High Order Differential Frequency Hopping: Design and Analysis. Hindawi Publishing Corporation Mathematical Problems in Engineering. Volume 2015. Article ID 586080. 9 pages. URL: <http://dx.doi.org/10.1155/2015/586080>.
16. Теорія електрозв'язку. Підручник: [у 2 т.]. Т. 2: Основи теорії завадостійкості, кодування та розподілу інформації / О. В. Корнейко, О. В. Кувшинов, О. П. Лежнюк, С. П. Лівенцев. Під ред. С. П. Лівенцева. К.: НВФ „Славутич-Дельфін”, 2006. 292 с.

ВИМОГИ ТА РЕЗУЛЬТАТИ ОЦІНКИ ЗАХИЩЕНОСТІ ПЕРСПЕКТИВНОГО ЕЛЕКТРОННОГО ПІДПISY ВІД СПЕЦІАЛЬНИХ АТАК

Виникнення нової ери криптографії – так званої постквантової або квантово безпечної – яка була б здатна протистояти атакам квантового обчислення, пов'язують з відкриттям алгоритму Шора у 1999 році. Цей алгоритм мав потенційну можливість зламати всі актуальні на той час схеми підписів. Як одне з ефективних постквантових рішень була запропонована криптографія на основі алгебраїчних решіток. Алгебраїчні решітки мають змогу протистояти навіть найсерйознішим криптоаналітичним атакам, оскільки задачі, засновані на припущеннях щодо решітки, забезпечують достатній показник захищеності від середніх до найгірших випадків (Ajtai та Dwork, 1997). До переваг роботи з решітками можна також віднести гомоморфне шифрування та шифрування на основі ідентичності. Підписам на решітках притаманні порівняно невеликі розміри ключів, підвищена швидкодія і, найголовніше – захищеність від квантових атак. Falcon є одним з трьох підписів на основі решітки серед учасників 2 раунду стандартизації NIST США.

Незважаючи на значні переваги, схеми на основі алгебраїчних решіток мають і недоліки. Основною проблемою є те, що постквантові схеми так само вразливі до атак бічними каналами, як і актуальні криптопримітиви. Саме тому слід враховувати можливі атаки та розглядати необхідні контрзаходи щодо них. На даний момент актуальними проти алгебраїчних решіток є часові атаки та атаки помилками. Тому це дослідження зосереджено саме на аналізі подібних атак на схему ЕП Falcon та можливих контрзаходах, які змогли б забезпечити захист від них. Головним зауваженням щодо Falcon, як до кандидата у другий раунд стандартизації, була непевність щодо його захищеності від атак бічними каналами. Це дослідження розглядає існуючі атаки на реалізацію та аналізує швидкодію схеми підпису з відповідними контрзаходами. Атака, яка буде розглядатися в даному дослідженні – BEARZ – є модифікацією атаки на геш-підписову схему DLP розроблену Espitau (Espitau та ін., 2016, 2018). Хоча відбірник алгоритму Falcon є вразливим до атак помилками, і це дає змогу отримати особистий ключ, ефективність компонентів даного алгоритму сприяє тому, що він є конкурентноспроможним, навіть при застосуванні контрзаходів. В середньому, у випадку схеми Falcon, контрзаходи викликають лише до 5% зниження ефективності. Одним з ефективних заходів проти запропонованої атаки помилками є нульова перевірка. Для набору параметрів з високою захищеністю подібний контрзахід спричиняє зниження продуктивності до 16 %.

СХЕМА ПІДПISY FALCON. Falcon – геш-підписова схема, яка заснована на шифруванні на основі DLP та методах швидкої вибірки Фур'є. Завдяки цим методам, вдається забезпечити невеликі розміри закритого ключа та підвищену швидкодію процедури вибірки. Генерація ключів відбувається за Алгоритмом 1 (рис. 1). Після генерації ключів, отримуємо NTRU-поліноми. При цьому f і g – особисті ключі, а $h = gf^{-1}$ – відкритий ключ.

Процес підписання показано в Алгоритмі 2 (рис. 1). Він відбувається шляхом знаходження короткого вектору в решітці NTRU з використанням закритого ключа. Для цього застосовується процедура *ffSampling* – показана в Алгоритмі 3 (рис. 2). Перевірка підпису виконується шляхом перевірки модуля, який розміщується в межах необхідної межі β , за допомогою відкритого ключа. Ця процедура показана в Алгоритмі 4 (рис. 2).

ЧАСОВІ АТАКИ НА FALCON. Деякі математичні компоненти, які використовуються в алгоритмі ЕП Falcon, є вразливими до атак, заснованих на аналізі часових показників. Це пов'язано з певними складнощами реалізації цих компонентів за постійний час.

ВІДБІРНИК ГАУСА. Саме Гаусові відбірники, як правило, є вразливим місцем для часових атак проти криптографії на решітках. Для схеми Falcon Гаусів відбірник виконує роль відбірника коротких векторів у решітках.

Algorithm 1: FALCON key generation (adapted from (Prest et al., 2017))

Data: N, q
Result: $\mathbf{B} \in \mathbb{Z}_q^{2N \times 2N}, h \in \mathcal{R}_q$

- 1 $\sigma_f = 1.17 \sqrt{\frac{q}{2N}}$
- 2 $f, g, \leftarrow \mathcal{D}_{N, \sigma_f}$
- 3 Norm
 $\leftarrow \max \left(\|g, -f\|, \left\| \left(\frac{q\tilde{f}}{f*f+g*g}, \frac{q\tilde{g}}{f*f+g*g} \right) \right\| \right)$
- 4 **if** Norm $> 1.17 \sqrt{q}$ **then** go to Step 2;
- 5 Compute $\rho_f, \rho_g \in \mathcal{R}$ and $R_f, R_g \in \mathbb{Z}$ such that:
 $\rho_f \cdot f = R_f$ and $\rho_g \cdot g = R_g$
- 6 **if** $\text{GCD}(R_f, R_g) \neq 1$ or $\text{GCD}(R_f, q) \neq 1$ **then**
go to Step 2;
- 7 Compute $u, v \in \mathbb{Z}$ such that: $u \cdot R_f + v \cdot R_g = 1$
- 8 $F \leftarrow qv\rho_g$ and $Q \leftarrow -qu\rho_f$
- 9 $k = \left\lfloor \frac{F*\tilde{f}+G*\tilde{g}}{f*f+g*g} \right\rfloor \in \mathcal{R}$
- 10 $F \leftarrow F - k*f$ and $G \leftarrow G - k*g$
- 11 $h = g * f^{-1} \bmod q$
- 12 $\mathbf{B} = \begin{pmatrix} g & -f \\ G & -F \end{pmatrix}$
- 13 $\hat{\mathbf{B}} = \begin{pmatrix} \text{FFT}(g) & -\text{FFT}(f) \\ \text{FFT}(G) & -\text{FFT}(F) \end{pmatrix}$
- 14 $T = \text{ffLDL}^*(G)$
- 15 $\sigma \leftarrow 1.55 \sqrt{q}$
- 16 **for** each leaf of T , leaf.value $= \sigma / \sqrt{\text{leaf.value}}$
- 17 $\text{sk} \leftarrow (\hat{\mathbf{B}}, T), \text{pk} = h$
- 18 **return** sk, pk

Algorithm 2: FALCON signing (adapted from (Prest et al., 2017))

Data: sk, $H : \{0, 1\}^* \rightarrow \mathbb{Z}_q^N, m, \beta$
Result: SIG_m

- 1 **if** SK_m is in local storage **then**
- 2 **return** Output SIG_m to message m
- 3 **else**
- 4 $r \leftarrow \text{Unif}(\{0, 1\}^{320})$
- 5 $c \leftarrow H(r||m)$;
- 6 $t \leftarrow (\text{FFT}(c), \text{FFT}(0)) \cdot \hat{\mathbf{B}}^{-1}$
 $z \leftarrow \text{ffSampling}(t, T)$
- 7 $s = (t - z)\hat{\mathbf{B}}$
- 8 **while** $\|s\| > \beta$
- 9 $(s_1, s_2) \leftarrow \text{invFFT}(s)$
- 10 $s_2 = \text{Compress}(s_2)$
- 11 $SIG_m \leftarrow (r, s_2)$
- 12 **return** Output SIG_m associated to message m and keep in local storage

Рисунок 1 – Алгоритми генерування підпису і підписування (Алгоритм 1 та 2)

Algorithm 3: ffSampling (Prest et al., 2017)

Data: $t = (t_0, t_1)$ in FFT format, T
Result: $z = (z_0, z_1)$ in FFT format

- 1 **if** $n = 1$ **then**
- 2 $\sigma' \leftarrow T.\text{value}$
- 3 $z_0 \leftarrow \mathcal{D}_{\mathbb{Z}, t_0, \sigma'}$
- 4 $z_1 \leftarrow \mathcal{D}_{\mathbb{Z}, t_1, \sigma'}$
- 5 **return** $z = (z_0, z_1)$
- 6 **else**
- 7 $(l, T_0, T_1) \leftarrow (T.\text{value}, T.\text{leftchild}, T.\text{rightchild})$
- 8 $\mathbf{t}_1 \leftarrow \text{splitfft}(t_1)$
- 9 $\mathbf{z}_1 \leftarrow \text{ffSampling}(\mathbf{t}_1, T_1)$
- 10 $z_1 \leftarrow \text{mergefft}(\mathbf{z}_1)$
- 11 $t'_0 \leftarrow t_0 + (t_1 - z_1) \cdot l$
- 12 $\mathbf{t}_0 \leftarrow \text{splitfft}(t'_0)$
- 13 $\mathbf{z}_0 \leftarrow \text{ffSampling}(\mathbf{t}_0, T_0)$
- 14 $z_0 \leftarrow \text{mergefft}(\mathbf{z}_0)$
- 15 **return** $z = (z_0, z_1)$

Algorithm 4: FALCON verifying (adapted from (Prest et al., 2017))

Data: $\text{pk} = h \in \mathcal{R}_q, (SIG_m, m), \beta$
Result: Accept or Reject

- 1 $c \leftarrow H(r||m)$
- 2 $s_2 = \text{Decompress}(s_2), s_1 \leftarrow c - s_2 h \bmod q$
- 3 **if** $\|(s_1, s_2)\| < \beta$ and $H(r||m) = c$ **then**
- 4 **return** Accept
- 5 **else**
- 6 **return** Reject

Рис. 2 Алгоритм ffSampling та алгоритм перевірки (Алгоритм 3 та 4)

ТЕОРЕТИЧНЕ ПЕРЕТВОРЕННЯ ЧИСЛА (NTT). NTT є потенційно вразливим до часових атак, оскільки використовує велику кількість модульної арифметики, яку важко реалізувати за постійний час. У схемі Falcon NTT використовується для пришвидшення множення кільцевих багаточленів.

HASH-TO-POINT. Процес гешування повідомлення до точки в кільці поліномів „може бути складно здійсненим при постійному часі” – зазначають автори алгоритму Falcon. Тому функція є потенційно вразливою до часових атак.

ЗАПРОПОНОВАНІ КОНТРЗАХОДИ ПРОТИ ЧАСОВИХ АТАК. Одним з ефективних на даний момент заходів проти часових атак є алгоритм BlindVector, запроваджений Saarinen (2017). У BlindVector покращено випадкові перемішування для протистояння атакам бічними каналами. Цей алгоритм використовується у даній реалізації, крім того гарантується постійна за часом реалізація навіть для подальшого збільшення складності атак. Для протидії часовим атакам, функції NTT та FFT також реалізовані постійними за часом. Це стає можливим

завдяки обробці всіх необхідних змінних гілки та відмови від логіки для більш тривалих арифметичних операцій. Для зменшення впливу на продуктивність даних контрзаходів, використовується „ледаче” скорочення (lazy reduction) та векторизація SIMD. Для забезпечення можливості виконання множення двох кілець у домені NTT застосовується поточкове модульне множення, яке забезпечує обчислення кожного елементу незалежно. Дані операції є послідовними та безумовними, тому можна говорити про їх усталеність у часі. Ще однією особливістю є те, що у перетворенні застосовується вдосконалений NTT алгоритм Cooley-Tukey. Покращення застосовуються для підвищення продуктивності, увімкнення автоматичної векторизації та гарантування того, що не використовуються умовні операції розгалуження. Також серед запропонованих заходів є відкидання вибірки. Даний контрзахід полягає в наступному – з випадкових адрес зчитується додатковий кеш з метою спотворити статистику для SCA і після цього зайві зчитування відкидаються. Діапазон норм відкидань у реалізації, що розглядається, обрано на рівні 6,25 %, 12,5 % та 25 %.

Ще одним нововведенням є ефективна конструкція методики гаусової вибірки (CDT) з постійним часом. Перевагою даної конструкції є чітка кількість операцій пошуку-зчитування, а також використання однакової арифметики, незалежно від гілки, обраної згідно з CDT. Верхня межа кількості необхідних пошукових операцій дорівнюватиме $\lceil \log_2 N \rceil$, тому кожен виклик пробовідбірника доповнюється до найближчого ступеня двійки для того, щоб виконати таку ж кількість тактових циклів.

АТАКА BEARZ НА FALCON. BEARZ – атака помилками на схему ЦП Falcon, запропонована Sarah McCarthy та ін. (2019). Принцип дії атаки полягає у вилученні базису через переривання рекурсії або обнулення. Атака добуває закриту ключову інформацію, шляхом спричинення помилок в роботі. Модель зловмисника передбачає, що він може пропускати команди та обнуляти змінні.

РЕКУРСІЯ АЛГОРИТМУ FALCON. Схема Falcon має два рекурсивні виклики на верхньому рівні алгоритму ffSampling. Для даного цільового вектора (t_0, t_1) , алгоритм діє спочатку на t_1 , рекурсивно, справа наліво, а потім на t_0 . Кожен елемент – t_1 і потім t_0 – безперервно ділиться на два вектори довжини $n := n/2$ поки n не буде дорівнювати 2, а потім відбирає коефіцієнти Гаусового розподілу, щоб отримати вектор вибірки (z_0, z_1) . Через це алгоритм верхнього рівня містить дві рекурсивні гілки. Зауважимо, що всі процедури виконуються в домені FFT. Для вектора довжини n , перші $n/2$ значень будуть представлені реальними коефіцієнтами, а другі $n/2$ – уявними. Спираючись на структуру рекурсії Falcon, для успішної атаки слід було б перервати рекурсивний виклик у необхідній точці, щоб тільки $m=n$ місць були б заповнені. На жаль це не є можливим через характер функцій FFT.

FFT: ЗЛИТТЯ ТА РОЗДІЛЕННЯ. Функції злиття та розділення для схеми Falcon виконуються у домені FFT. Це спричиняє проблему для атаки помилками, оскільки нульові вхідні дані не представлені нулем у FFT. Тому є необхідність відстеження коефіцієнтів зразків під час руху вгору по рекурсивному дереву. Після отримання вектору решітки із Гаусового зразка, до нього застосовується зворотна функція FFT (FFT^{-1}). Це необхідно, щоб переконатися, що підпис не знаходиться в домені FFT. Після цього може бути використана та сама після-обробка, що і для DLP-атаки. Атаки шляхом переривання рекурсії можна класифікувати, в залежності від місця переривання. Але усі методи атаки призводять до однакового вихідного векторного формату для z ; перші $(2n-m)$ коефіцієнтів $z = (z_0, z_1)$ примусово задаються нулями.

ПЕРЕРИВАННЯ ДРУГОЇ РЕКУРСІЇ (ДЛЯ $m=n$). Атака полягає в перериванні виклику алгоритму вибірки в кінці, після першого рекурсивного виклику (рядок 10 алгоритму 3). Після виконання атаки z_1 заповниться вибраними коефіцієнтами, а z_0 залишиться повністю нульовим. Це також можна виконати для $m \leq n$, з метою обнулення перших n коефіцієнтів.

ОБНУЛЕННЯ АБО АТАКА ПРОПУСКУ (ДЛЯ $m \leq n$). Можливі два варіанти даної атаки. Перший – при передостанньому злитті ($n =$ від 256 до 512), встановити необхідні

(наприклад, перша половина, якщо $m = n/2$) з вихідних коефіцієнтів в нуль шляхом пропуску операцій або обнулення. Операції, що пропускаються: $f[(u \ll 1) + 0] = t_re$ і $f[(u \ll 1) + 1] = t_re$, з коду (Prest та ін., 2017) (*merge_fft()* функція у *falcon_fft.c*). Другий – встановити необхідну кількість перших коефіцієнтів z_1 в нуль перед обчисленням відповідного вектора решітки, тобто перезаписати вихід відбірника – z_1 .

ПЕРЕРИВАННЯ СЕРЕДНЬОЇ РЕКУРСІЇ ($m \leq n$). Даний тип атаки вимагає одноразового попереднього обчислення, проте дозволяє застосовувати помилку на стадії одновимірного Гаусового відбірника, що сприяє простоті фізичного вбудовування. Якщо нам необхідно прирівняти до нуля ліву половину z_1 ($m = n/2$), то вектор лівої сторони (LHS) при останньому виклику *merge_fft()* повинен містити у першій половині нульові значення, а у векторі правої сторони (RHS) перша половина коефіцієнтів має бути рівною другій половині. Кожен реальний коефіцієнт вектору z_1 генерується як $z_1[2u] = f_0[u] + (f_1[u] - f_1[u + n/4])$ та $z_1[2u+1] = f_0[u] + (f_1[u] - f_1[u + n/4])$, де n – розмірність вектора вищого рівня, і $u \in \{0, \dots, n/4-1\}$. Для того, щоб прирівняти $z_1[2u]$ і $z_1[2u+1]$ до нуля, встановлюється $f_0[u] = 0$ і $f_1[u] = f_1[u + n/4]$ для кожного $u \in \{0, \dots, n/4-1\}$. Тому, наприклад, для $n = 512$, перші $n/4 = 128$ коефіцієнтів 256-мірного вектора LHS встановлюються рівними нулю, а перші 128 коефіцієнтів 256-мірного вектора RHS встановлюються рівними другим 128 коефіцієнтам цього ж вектора.

Щодо 256-розмірного RHS вектору – він повинен містити в першій половині значення, рівні значенням другої половини. Щоб це могло статися, 128-мірний вектор LHS повинен мати реальні значення, що дорівнювали б уявним значенням, а 128-розмірний RHS вектор повинен бути нульовим. Це зумовлено тим, що необхідно отримати $f[2u] = f[2u + n/2]$ та $f[2u+1] = f[2u+1 + n/2]$ рівним для кожної ітерації u . Функція *merge_fft()* виконує це наступним чином: $f_0[u] + (f_1[u] - f_1[u + n/4]) = f_0[u + n/4] + (f_1[u] + f_1[u + n/4])$ і $f_0[u] - (f_1[u] - f_1[u + n/4]) = f_0[u + n/4] - (f_1[u] + f_1[u + n/4])$. Щоб умова вище виконувалася, встановлено наступні правила $f_0[u] = f_0[u + n/4]$ – перша половина коефіцієнтів дорівнюватиме другій половині, і $f_1[u] = f_1[u + n/4] = 0$. Тому рівняння будуть просто залежати від вектора подачі LHS. Для RHS кожену нижню гілку можна встановити в нуль. Візьмемо LHS 128-розмірний вектор: 64-мірний вектор LHS повинен мати рівні реальні та уявні значення, а RHS має бути нульовим. Будь-який рівний нулю вектор повинен мати обидва вектори подачі рівними нулю, тому гілки нижче цієї можуть бути обнулені. Цей метод може застосовуватися для будь-якого m такого, що $m = 2^k$, де $k \in \mathbb{Z}$.

ОБРОБКА ПІСЛЯ АТАКИ. Після отримання недійсного підпису атака передбачає відновлення таємного базису з нього. Наприклад, у нас маєтись $2n - m$ коефіцієнтів вектора (z_0, z_1) , які дорівнюють нулю. Тоді обчислюємо підпис Falcon s_2 як:

$$s = t - zB$$

де B – базова матриця в домені FFT. Але нам потрібна лише друга половина $s - s_2$, де:

$$s_2 = t_1 - z \begin{pmatrix} -A(f) \\ -A(F) \end{pmatrix}$$

і так як t_1 встановлено в нуль:

$$s_2 = -z \begin{pmatrix} -A(f) \\ -A(F) \end{pmatrix}.$$

Крім того, перші $m - n$ коефіцієнтів z дорівнюють нулю, що означає:

$$s_2 = -z_1(-A(F))$$

і оскільки деякі з коефіцієнтів z_1 дорівнюють нулю, нарешті маємо:

$$s_2 = (z_1[m-1]x^{n-m}F + \dots + z_1[0]x^{n-1}F).$$

Тим самим отримується підрешітка решітки, згенерованої за допомогою F . Таким чином, з кількома недійсними підписами можна знайти решітку, породжену F (де F є коротким вектором у цій решітці), а завдяки алгоритму BKZ можна знайти цей короткий вектор. Після цього G, f, g можна отримати з відкритого ключа h , і таким чином можна знайти таємний базис NTRU решітки.

РЕЗУЛЬТАТИ АТАКИ. Після успішного виконання всіх тестів, було зібрано 1 недійсних підписів для m значень нулів, наведених в таблиці 2. Для отримання полінома особистого ключа F було застосовано алгоритм BKZ (FPLLL Development Team, 2016). Таблиця 1 містить часові результати запуску алгоритмів.

Таблиця 1 – Часи (у секундах) на застосування алгоритму BKZ для 1 недійсних підписів для отримання базового полінома F (працює на одному ядрі процесора Intel Core i7-6700HQ на частоті 2,60 ГГц)

Набір параметрів	m	l=m+1	l=m+2	l=m+3
Набір 1	64	0.07	0.07	0.08
	128	0.35	0.30	0.36
	256	2.17	2.80	2.36
Набір 2	128	0.28	0.29	0.35
	256	2.24	2.55	2.67

МОДЕЛЬ ПОМИЛКИ. Модель помилки передбачає аналіз бічних каналів, завдяки якому може бути виявлено вікно між першим і другим рекурсивним викликом. В межах цього вікна алгоритм може бути перервано. Для застосування атаки обнуленням можна використати момент зберігання вектору в оперативній пам'яті, обнуливши під час цього необхідні біти (Naccache та ін., 2005). Як альтернативу можна розглядати пропуск рядків. Його можна виконати за допомогою перепадів тактової частоти процесора (Blömer та ін., 2014).

КОНТРЗАХОДИ ПРОТИ BEARZ. Для запобігання атаці BEARZ існують певні контрзаходи. Одним з найпростіших методів виявлення атак помилками є подвійне обчислення підпису. Це подвоює час підписання. При перевірці відразу після підписування підписувач може переконатися в тому, що обладнання не піддавалося атакам помилками (Bruinderink та Pessl, 2018). Також простим та ефективним методом виявлення BEARZ атаки є перевірка того, що вибраний вектор не йде до нуля в певній точці вздовж своєї довжини в кінці ffSampler алгоритму.

FALCON 3 КОНТРЗАХОДАМИ

Implementation	Parameters	KeyGen	Sign	Verify	% decrease
Reference (Prest et al., 2017)	Set 1	143	6081.9	37175.3	-
Intel Core i7-6567U @ 3.3GHz	Set 2	50.9	3072.5	17697.4	-
Baseline	Set 1	29.8	1484	29002	-
+constant-time NTT	Set 2	11.1	734	14366	-
+Verify-after-sign	Set 1	-	1412	-	5
	Set 2	-	699	-	5
+Zero-check	Set 1	-	1006	-	32
	Set 2	-	489	-	16
+Double Computation +Verify after sign	Set 1	-	706	-	52
	Set 2	-	350	-	76
+Sample Discard (Low) (6.25%)	Set 1	26.3	-	-	12
	Set 2	12.0	-	-	+8
+Sample Discard (Medium) (12.5%)	Set 1	24.9	-	-	16
	Set 2	10.2	-	-	8
+Sample Discard (High) (25%)	Set 1	27.7	-	-	7
	Set 2	8.0	-	-	28
+Fisher-Yates Shuffling	Set 1	23.87	-	-	20
	Set 2	10.9	-	-	2
+BlindVector	Set 1	27.03	-	-	9
	Set 2	8.7	-	-	49
+Verify-after-sign +Sample Discard (Low) (6.25%) +Fisher-Yates Shuffling	Set 1	29.0	1426	-	4
	Set 2	10.7	706	-	4

Рис. 3 Результати продуктивності для Falcon із контрзаходами SCA, включаючи відсоткове зменшення задіяних компонентів, на Intel E5-1620 при 3,7 ГГц (якщо не вказано інше)

Як видно з рис. 3 – контрзаходи не мають значного впливу на швидкодію Falcon. Загальна рекомендована комбінація контрзаходів уповільнює генерацію ключів та

підписання менш, ніж на 5% для набору параметрів 1. Такий результат зумовлений ефективністю процесів вибірки та перевірки.

ЧАСОВІ АТАКИ. Для перевірки контрзаходу проти атак помилками, було 100 разів проведено процедуру підписання та визначено, що для набору 1, він потрапляв в діапазон 50 операцій на секунду, а для набору 2 – 20 операцій на секунду. Це свідчить про його ефективність проти часових атак.

АТАКА BEARZ. Перевірка після підписування може не виявити атаки помилками, яка націлена на вибірку, якщо одна і та ж помилка успішно реалізована двічі. Тому атака все ще може сформувати дійсний підпис і залишитись невиявленою. Однак контрзахід нульової перевірки повинен виявити атаку зі 100% успіхом. Тому його можна рекомендувати як мінімальний і достатній контрзахід.

ПОРІВНЯННЯ З ІНШИМИ СХЕМАМИ ПІДПИСІВ НА ОСНОВІ РЕШІТКИ. У цьому підрозділі проводиться порівняння результатів даної реалізації Falcon з Dilithium (Lyubashevsky та ін., 2017) та Bliss-B (Ducas, 2014) з використанням запропонованих контрзаходів. Застосування перевірки після підпису спричиняє менші втрати продуктивності для алгоритму Falcon порівняно з алгоритмом Dilithium, як показано на рис. 5. Навіть при високому рівні безпеки його продуктивність знижується не так помітно, як у BLISS-B, як показано на рис. 4. Це можна пояснити ефективністю компонентів алгоритму ЕП Falcon.

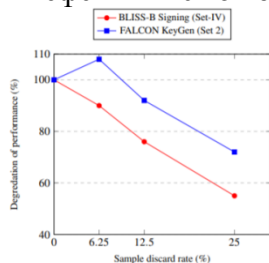


Рис. 4 Ефект контрзаходу відкидання зразків на BLISS-B та Falcon для відповідного (192 біти) рівня захищеності

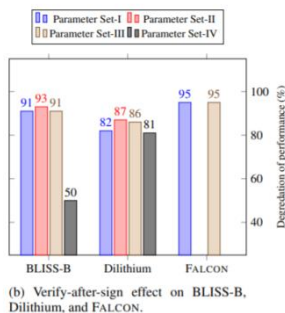


Рис. 5 Ефект перевірки після підпису на BLISS-B, Dilithium та Falcon

BLISS-B пропонує широкий спектр контрзаходів для захисту від запропонованих атак, і, як видно з рис. 5, їх вплив на продуктивність може коливатися від додаткових 10 % до 50 %, залежно від реалізації. Однією з переваг схеми Dilithium є захищеність від атак на відбірник Гауса, проте його захист від атак помилками Bruinderink та Pessl (2018) залишається проблемою. При застосуванні до нього контрзаходів, його ефективність сповільнюється майже на 20 %. А це є навіть гіршими показниками, ніж показники BLISS-B при застосуванні контрзаходу для захисту Гаусового відбірника. У цьому дослідженні було розглянуто атаку на схему підпису Falcon – BEARZ. Було показано, що певні математичні компоненти, які використовуються в алгоритмі ЕП Falcon, є вразливими до атак, заснованих на аналізі часових показників, а також, що Falcon є вразливим до атак помилками на відбірник Гауса. Через це при стандартизації чи впровадженні слід розглядати можливість фізичних атак. Було розглянуто можливі контрзаходи для протидії спеціальним атакам, показано вплив даних контрзаходів на швидкодію алгоритму. Крім того, було порівняно швидкодію різних схем, заснованих на решітках, і показано, що Falcon є конкурентним кандидатом другого раунду, навіть із застосуванням запропонованих контрзаходів.

ПАРАМЕТРИ ТА ОБҐРУНТОВАНІСТЬ ЇХ ВИБОРУ ДЛЯ АЛГОРИТМУ ЕП RAINBOW

Щоб гарантувати безпечність комунікації, важливо мати швидкі та надійні схеми підпису. Однією з основних областей їх застосування є автентичність даних та інформації, наприклад, оновлення програмного забезпечення. Одним з найбільш перспективних кандидатів у цій області є схема підпису Rainbow, яку запропонували J. Ding та D. Schmidt [1], яка є дуже ефективною та забезпечує швидку генерацію та перевірку підписів. В протилежність класичним схемам, таким як RSA чи EC-DSA, вважається, що Rainbow захищений від атак, що здійснюються за допомогою квантових комп'ютерів [2]. За останні роки було зроблено чимало роботи з дослідження безпечності багатовимірних схем та запропоновано чимало атак. Серед них прямі атаки [3 – 4], а також рангові атаки, котрі було введено Coppersmith та Stern [5] для атаки на схему Birational Permutation і пізніше покращено рядом інших дослідників [6 – 7]. Детальніше огляд цих атак запропоновано у [8]. Спеціальні атаки на схеми подібні до Rainbow були запропоновані Ding та Yang у [9]. Також робилися спроби вивести відповідні параметри зі складності цих атак у [10]. Однак, до сих пір залишається відкритою проблема адаптації параметрів багатовимірних схем до майбутніх розробок в області криптоаналізу та обчислювальних потужностей. У цій доповіді буде виконано спробу дослідження цього питання для схеми підпису Rainbow. Для цього ми розглянемо відомі атаки на схему підпису Rainbow. Як результат, наведемо порівняння з точку зору розмірів ключів та довжини підписів для рекомендованих системних параметрів.

ОСНОВНІ ПАРАМЕТРИ ЕП RAINBOW. До основних системних параметрів алгоритму електронного підпису (ЕП) Rainbow належать наступні змінні:

кінцеве поле $F = F_q$ з елементами q

цілі числа $0 < v_1 < \dots < v_u < v_{u+1} = n$

множина індексів $V_i = \{1, \dots, v_i\}$, $O_i = \{v_i + 1, \dots, v_{i+1}\}$ ($i = 1, \dots, u$). Зверніть увагу, що

кожний $k \in \{v_1 + 1, \dots, n\}$ міститься рівно в одному з наборів O_i . ($v > u$)

маємо $|V_i| = v_i$ та множину $o_i := |O_i|$ ($i = 1, \dots, u$)

кількість рівнянь: $m = n - v_1$

кількість змінних: n

У наведеному прикладі змінними v та u є незбалансовані поліноми Oil-Vinegar або їх відповідні коефіцієнти, кількість яких залежить від інших параметрів (n та m , відповідно). У документації Rainbow пропонується наступні три набори параметрів:

Ia (F, v_1, o_1, o_2) = (GF(16), 32, 32, 32) (64 рівняння, 96 змінних)

IIIc (F, v_1, o_1, o_2) = (GF(256), 68, 36, 36) (72 рівняння, 140 змінних)

Vc (F, v_1, o_1, o_2) = (GF(256), 92, 48, 48) (96 рівняння, 188 змінних)

Запропоновані набори параметрів зазначаються наступним чином: римська цифра вказує на категорію безпеки NIST, на яку націлено конкретний екземпляр Rainbow. Літера вказує на кінцеве поле, що використовується у схемі (а для GF(16) та с для GF(256)). Зверніть увагу, що кожен з двох наборів параметрів задовольняє вимогам двох категорій безпеки NIST. Зокрема, екземпляр Rainbow Ia задовольняє вимогам безпеки категорій I та II, набір параметрів IIIc – III та IV, а Vc – V та VI. Для кожного з трьох наборів параметрів пропонується стандартний, циклічний та стислий варіант відповідного екземпляра Rainbow.

АТАКИ НА СХЕМУ RAINBOW. У цьому розділі розглядаються найбільш популярні атаки на схему цифрового підпису Rainbow та формулювання до показників безпеки відштовхуючись від системних параметрів та очікуваного рівня безпеки.

АТАКИ НА ГЕШ-ФУНКЦІЮ. Так як схема ЕП Rainbow дотримується підходу Hash-then-Sign, вона може бути атакована шляхом знаходження колізій у використовуваній геш-функції. У цій роботі не розглядаються конкретні атаки на геш-функцію, але розглядається використовувана геш-функція H як ідеальна випадкова функція $H : \{0, 1\}^* \rightarrow F^m$.

Тому, щоб попередити (класичну) атаку на геш-функцію, що використовується у схемі Rainbow, кількість m рівнянь у публічній системі Rainbow повинно бути обрано таким, щоб $m \cdot \log_2 q \geq \text{seclev}$,

де q – кардинальність кінцевого поля, а seclev – необхідний рівень безпеки. Іншими словами, щоб попередити атаки на геш-функцію, що використовується, кількість m рівнів у відкритому ключі (та центральній карті) Rainbow повинно бути обране, щонайменше, наступним чином

$$m \geq \frac{2 \cdot \text{seclev}}{\log_2 q}.$$

Обираючи m таким чином ми гарантуємо, що (класична) атака колізії на геш-функцію у схемі Rainbow потребує щонайменше 2^{seclev} обчислень геш-функції H .

ПРЯМІ АТАКИ. Найпростішою атакою на багатовимірні схеми, такі як Rainbow, є пряма алгебраїчна атака, у якій відкрите рівняння $P(\mathbf{z}) = \mathbf{h}$ розглядається як приклад MQ-проблеми. Оскільки відкрита система Rainbow є недостатньо визначеною системою з $n \approx 1.5 \cdot m$, найбільш ефективним способом вирішення цього рівняння є фіксація $n - m$ змінних для створення детермінованої системи перед використанням алгоритму, такого як XL або техніки Grobner Basis таких як F_4 або F_5 [11]. Можна очікувати, що результуюча детермінована система має рівно один розв'язок. У деяких випадках можна отримати ще кращі результати при вгадуванні додаткових змінних до вирішення системи (гібридний підхід) [12]. Складність вирішення такої системи m квадратичних рівнянь з m змінними використовуючи підхід XL Wiedemann можна оцінити як

$$\text{Complexity}_{\text{direct; classical}} = \min_k \left(q^k \cdot 3 \cdot \binom{m-k+d_{\text{reg}}}{d_{\text{reg}}}^2 \cdot \binom{m-k}{2} \right)$$

множень поля, де d_{reg} – так звана ступінь регулярності системи. Як показали експерименти, публічні системи Rainbow ведуть себе майже як випадкові системи. Таким чином, ми можемо оцінити степінь регулярності як найменше ціле число d , для якого коефіцієнт t^d

$$\frac{(1-t^2)^m}{(1-t)^{m-k}}$$

не додатній. За наявності квантових комп'ютерів додатковий етап вгадування гібридного підходу може бути пришвидшено алгоритмом Гровера. Таким чином, ми можемо оцінити складність квантової прямої атаки по множенню полів

$$\text{Complexity}_{\text{direct; quantum}} = \min_k \left(q^{k/2} \cdot 3 \cdot \binom{m-k+d_{\text{reg}}}{d_{\text{reg}}}^2 \cdot \binom{m-k}{2} \right).$$

Тут значення d_{reg} можна вирахувати так, як було зазначено вище.

АТАКА МІНІМАЛЬНОГО РАНГУ (MINRANK). У атаці MinRank [13] атакуючий намагається знайти лінійну комбінацію публічних поліномів мінімального рангу. У випадку з Rainbow така лінійна комбінація рангу v_2 відповідає лінійній комбінації центральних поліномів першого шару. Таким чином, знайшовши o_1 з цих рангових комбінацій, можна визначити центральні поліноми першого шару та відтворити еквівалентний особистий ключ

Rainbow. Як показано у роботі Billet та ін. [13], цей крок може бути виконаний за допомогою множення полів

$$Complexity_{MinRank; classical} = q^{v_1+1} \cdot m \cdot \left(\frac{n^3}{3} - \frac{m^2}{6} \right). \quad (1)$$

Використовуючи алгоритм Гровера на етапі пошуку, ми можемо зменшити складність до множення полів

$$Complexity_{MinRank; quantum} = q^{\frac{v_1+1}{2}} \cdot m \cdot \left(\frac{n^3}{3} - \frac{m^2}{6} \right). \quad (2)$$

Існує альтернативне формулювання атаки MinRank, так зване Minors Modeling. У цьому формулюванні задача MinRank вирішується шляхом розв'язання системи нелінійних поліноміальних рівнянь (заданих $v_2 + 1$ молодшими значеннями матриці, що представляють необхідну лінійну комбінацію). Складність даної атаки можна оцінити як

$$Complexity_{MinRank; Minors} = \binom{n+v_2+1}{v_2+1}^{\omega},$$

де $2 < \omega \leq 3$ – постійна лінійної алгебри при розв'язку системи лінійних рівнянь.

Однак у випадку з Rainbow ця складність вища, ніж у випадку з MinRank-атакою, яка використовує методи лінійної алгебри (див. рівняння (1)). Більше того, оскільки ми маємо справу з сильно детермінованою системою, атака MinRank з використанням Minors Modeling не може бути пришвидшена квантовими методами. Тому при аналізі безпеки наших екземплярів Rainbow, ми використовуємо рівняння (1) та (2) для оцінки складності атаки MinRank.

АТАКА ВИСОКОГО РАНГУ (HIGHRANK). Ціллю атаки HighRank [14] є ідентифікація (лінійне уявлення) змінних, що з'являються найменшу кількість разів у центральних поліномах (вони відповідають Oil-змінним останнього шару Rainbow, тобто змінні x_i для $i \in O_u$). Складність цієї атаки можна оцінити як

$$Complexity_{HighRank; classical} = q^{O_u} \cdot \frac{n^3}{6}.$$

За наявності квантових комп'ютерів ми можемо пришвидшити крок пошуку за допомогою алгоритму Гровера. Так ми отримаємо множення полів

$$Complexity_{HighRank; quantum} = q^{O_u/2} \cdot \frac{n^3}{6}.$$

UOV АТАКА. Оскільки Rainbow можна розглядати як розширення добре відомої схеми підписів Oil та Vinegar [15], вона може бути атакована з використанням усіх відомих атак UOV. Зокрема, атака Reconciliation [16] та атака UOV “Oil Subspace” Kipnis та Shamir [17], з яких найбільш серйозною є остання. Rainbow розглядається як екземпляр UOV з $v = v_1 + o_1$ та $o = o_2$. Метою атаки є пошук попереднього образу, який називається підпростором Oil O під афінним перетворенням T , де $O = \{x \in F^n : x_1 = \dots = x_v = 0\}$. Пошук цього простору дозволяє відокремити oil змінні від vinegar та відновити особистий ключ.

Складність цієї атаки можна оцінити як множення полів

$$Complexity_{UOV-Attack; classical} = q^{n-2o_2-1} \cdot o_2^4.$$

Використовуючи алгоритм Гровера, ця складність може бути зведена до множення полів

$$Complexity_{UOV-Attack; quantum} = q^{\frac{n-2o_2-1}{2}} \cdot o_2^4.$$

АТАКА З РОЗДІЛОМ СМУГ RAINBOW (RAINBOW-BAND-SEPARATION). Атака Rainbow-Band-Separation [16] націлена на пошук лінійних перетворень S та T , що перетворюють відкриті поліноми у поліноми форми Rainbow (тобто Oil $\times$ Oil членів повинні

бути рівні нулю). Для цього зломисник повинен вирішити декілька нелінійних багатовимірних систем. Складність цього кроку визначається складністю вирішення першої (та найбільшої) з цих систем, яка складається з $n+m-1$ квадратичних рівнянь з n змінних. Так як ця система є перевантаженою (рівнянь більше, ніж змінних), то зазвичай ми не досягаємо прискорення намагаючись вгадати змінні перед застосуванням алгоритмів типу XL. Однак, щоб бути вичерпним, розглядається саме гібридний підхід у оцінці складності. Таким чином ми отримаємо

$$Complexity_{RBS;classical} = \min_k \cdot q^k \cdot 3 \cdot \binom{n+d_{reg}-k}{d_{reg}} \cdot \binom{n-k}{2}$$

множень у полі. Знову ж таки, багатовимірні квадратичні системи, генеровані цією атакою, поводять себе дуже схоже на випадкові системи. Тому ми можемо оцінити значення d_{reg} , як

$$\frac{(1-t^2)^{m+n-1}}{(1-t)^{n-k}}$$

найменше ціле число d , для якого коефіцієнт t^d у не є додатнім. Використовуючи алгоритм Гровера ми можемо пришвидшити крок здогадування гібридного підходу. Зробивши це, ми отримаємо

$$Complexity_{RBS;quantum} = \min_k \cdot q^{k/2} \cdot 3 \cdot \binom{n+d_{reg}-k}{d_{reg}} \cdot \binom{n-k}{2}$$

множень у полі. Значення d_{reg} може бути оцінено як вказано вище. Однак, так як оптимальне число k змінних, що вгадуються на протязі атаки, дуже мале (у більшості випадків воно дорівнює 0), вплив квантового прискорення на складність атаки Rainbow-Band-Separation досить обмежено.

КВАНТОВА АТАКА ГРУБОЇ СИЛИ (QUANTUM BRUTE-FORCE-ATTACKS)

За наявності квантових комп'ютерів атаку грубої сили на схему можна значно пришвидшити з використанням алгоритму Гровера. Наприклад, у [18] було показано, що двійкова система з m рівнянь та m змінних може бути вирішена за допомогою

$$2^{m/2} \cdot 2 \cdot m^3$$

бітових операцій. Загалом, завдяки алгоритму Гровера ми очікуємо квадратичної швидкості атаки грубої сили. Тому, для досягнення рівня безпеки у secl_v біт, нам знадобиться щонайменше

$$m \geq \frac{2 \cdot \text{secl}_v}{\log_2 q}$$

рівнянь. Однак, цієї умови вже достатньо для попередження атак на геш-функцію. Тому ми не розглядаємо атаки з використанням квантової грубої сили для вибору параметрів у екземплярах Rainbow. У формулах, що наведені в цьому розділі, даються оцінки складності атак з точки зору їх багаторазового множення у полі. Щоб перевести ці складності до підрахунку кількості операцій, як це пропонується у специфікації NIST, ми робимо наступні припущення: множення одного поля у полі $GF(q)$ вимагає приблизно $\log_2(q)^2$ біт множення (операція AND) та таку ж кількість складань (операція XOR). для кожного множення полів, що виконуються у процесі атаки, також вимагається додавання елементів поля. Кожне з цих додавань вимагає $\log_2(q)$ бітових складень (XOR). Таким чином, кількість операцій, що вимагаються для атаки, можна обчислити як

$$\# gates = \# field multiplications \cdot (2 \cdot \log_2(q)^2 + \log_2(q)).$$

ПОРІВНЯННЯ ТА РЕКОМЕНДАЦІЇ. У [19], за допомогою ефективної реалізації алгоритму Faugeres F4 [7] у середовищі MAGMA для обчислення Grobner-базисів, вивчається складність атак у полях GF(16), GF(31) та GF(256), заради знаходження рекомендованих параметрів для схеми Rainbow. Набір запропонованих параметрів є досить великим за обсягом для наведення у цій доповіді, тому нижче, у таблиці 1, буде наведено запропонований авторами набір параметрів, на основі якого виконувалось порівняння основних характеристик алгоритму ЕП. Ми наведемо порівняння розмірів ключів та довжин підписів для рекомендованих параметрів залежно від цільового рівня безпеки, який відображено певною датою. Таблиця 1 – Наведення основних системних параметрів для відповідного рівня безпеки

GF	Рік	Розмір гешу (біт)	(m, n)	Розмір ВК (кБ)	Приклад схеми (v_1, o_1, o_2)	Розмір ОК (кБ)	Розмір підпису (біт)	ІМУ (Нездійснення кількість Мірс-років)
16	2010	160	(40,61)	38.1	(21,20,20)	26.4	244	$1.45 \cdot 10^{12}$
	2020	192	(48,73)	65.0	(25,24,24)	44.2	292	$2.94 \cdot 10^{14}$
	2030	224	(56,85)	102.3	(29,28,28)	68.6	340	$5.98 \cdot 10^{16}$
	2040	248	(62,94)	138.0	(32,31,31)	91.8	376	$1.22 \cdot 10^{19}$
	2050	280	(70,106)	197.5	(36,35,35)	130.1	424	$2.47 \cdot 10^{21}$
31	2010	160	(33,52)	30.7	(19,16,17)	22.2	280	$1.45 \cdot 10^{12}$
	2020	192	(39,58)	44.9	(19,20,19)	30.7	312	$2.94 \cdot 10^{14}$
	2030	224	(46,67)	61.1	(21,24,22)	46.6	360	$5.98 \cdot 10^{16}$
	2040	248	(51,76)	89.9	(25,26,25)	66.5	408	$1.22 \cdot 10^{19}$
	2050	280	(57,85)	138.8	(28,29,28)	91.8	456	$2.47 \cdot 10^{21}$
256	2010	208	(26,43)	25.7	(17,13,13)	19.1	344	$1.45 \cdot 10^{12}$
	2020	256	(32,53)	47.3	(21,16,16)	34.4	424	$2.94 \cdot 10^{14}$
	2030	304	(38,65)	84.0	(27,19,19)	60.5	520	$5.98 \cdot 10^{16}$
	2040	344	(43,74)	122.6	(31,21,22)	87.7	592	$1.22 \cdot 10^{19}$
	2050	392	(49,85)	183.3	(36,24,25)	130.2	680	$2.47 \cdot 10^{21}$

РОЗМІРИ КЛЮЧІВ. У таблиці 2 показані розміри відкритих ключів для схеми Rainbow над полями GF(16), GF(31) та GF(256). Таблиця 2 – Розмір відкритих ключів Rainbow над різними полями (у кБ)

Рік	GF(16)	GF(31)	GF(256)
2010	38,1	30,7	25,7
2020	65,0	44,9	47,5
2030	102,3	72,3	84,0
2040	138,0	99,7	122,6
2050	197,5	138,8	183,3

На даний момент розміри ключів мінімальні для схем Rainbow над GF(256), але їх зростання набагато швидше, ніж відповідні розміри ключів над полем GF(31). Таким чином, починаючи з 2018 року, найменшими за розміром будуть ключі схем Rainbow над полем GF(31). ДОВЖИНА ПІДПISУ.

ік	F(16)	F(31)	F(256)	с
010	44	80	44	3
020	92	12	24	4
030	40	60	20	5
040	76	08	92	5
050	24	56	80	6

Таблиця 3 порівнює схему Rainbow над полями GF(16), GF(31) та GF(256) з точки зору довжини підпису. Як видно з таблиці, при використанні Rainbow над полем GF(16) виходять найкоротші підписи. Ці підписи приблизно на 20-30 біт коротші, ніж ті, що виходять у полі GF(31). Підписи Rainbow над GF(256) набагато довші і ця різниця у довжині буде збільшуватися з плином часу.

Таблиця 3 – Довжина підпису Rainbow над різними полями (у бітах)

ВИСНОВКИ. У даній роботі було наведено вимоги до основних системних параметрів з точки зору розгляду основних атак, що можуть бути використані для схем ЕП на багатовимірних перетвореннях та безпосередньо на алгоритм Rainbow, а також наведено порівняння основних характеристик підпису (розмір ключа та довжина підпису) при використанні відповідного набору рекомендованих системних параметрів.

ЛІТЕРАТУРА

1. Ding J., Schmidt D.: Rainbow, a new multivariate polynomial signature scheme. In Ioannidis, J., Keromytis, A.D., Yung, M. (eds.) ACNS 2005. LNCS vol. 3531, pp. 164–175 Springer, Heidelberg (2005).
2. Bernstein, D.J., Buchmann, J., Dahmen, E. (eds.): Post Quantum Cryptography. (2009).
3. Yang, B.-Y., Chen J.-M.: All in the XL family: Theory and practice. In LNCS 3506 pp. 67–86. Springer, Heidelberg (2007).
4. Faugere, J.C.: A new efficient algorithm for computing Groebner bases (F4). Journal of Pure and Applied Algebra, 139:61–88 (1999).
5. Coppersmith, D., Stern, J., Vaudenay, S.: Attacks on the Birational Signature Scheme. In LNCS 773 pp. 435 to 443, Springer, Heidelberg (1994).
6. Yang, B.-Y., Chen J.-M.: Building secure tame like multivariate public-key cryptosystems: The new TTS. In: Boyd, C., Gonzales Nieto, J.M. (eds.) ACISP 2005. LNCS vol. 3574, pp. 518–531. Springer, Heidelberg (2005).
7. Billet, O., Gilbert, H.: Cryptanalysis of Rainbow. In DePrisco, R., Yung, M. (eds.) SCN 2006, LNCS vol. 4116, pp. 336–347. Springer, Heidelberg (2006).
8. Goubin, L. and Courtois, N.T.: Cryptanalysis of the TTM cryptosystem. In Advances in Cryptology ASIACRYPT 2000, LNCS vol. 1976, pp. 44 – 57. Tatsuaki Okamoto, ed., (2000).
9. Ding, J., Yang, B.-Y., Chen, C.-H. O., Chen, M.-S., and Cheng, C.M.: New Differential-Algebraic Attacks and Reparametrization of Rainbow. In: LNCS 5037, pp.242 – 257, (2005).
10. Chen, A.I.-T., Chen, C.-H. O., Chen, M.-S., Cheng, C.M., and Yang, B.-Y.: Practical-Sized Instances for Multivariate PKCs: Rainbow, TTS and ℓ IC- Derivatives. In: LNCS 5299 pp. 95–108, Springer Heidelberg (2008).
11. J.-C. Faugère: A new efficient algorithm for computing Gröbner Bases (F4). Journal of Pure and Applied Algebra, 139:61 – 88, 1999.
12. L. Bettale, J.-C. Faugère, L. Perret: Hybrid approach for solving multivariate systems over finite fields. Journal of Mathematical Cryptology, 3: 177-197, 2009.
13. O. Billet, H. Gilbert. Cryptanalysis of Rainbow: SCN 2006, LNCS vol. 4116, pp. 336 - 347. Springer, 2006.
14. D. Coppersmith, J. Stern, S. Vaudenay: Attacks on the birational signature scheme. CRYPTO 1994, LNCS vol. 773, pp. 435 – 443. Springer, 1994.
15. A. Kipnis, J. Patarin, L. Goubin: Unbalanced Oil and Vinegar schemes. EUROCRYPT 1999, LNCS vol. 1592, pp. 206 – 222. Springer, 1999.
16. J. Ding, B.-Y. Yang, C.-H. O. Chen, M.-S. Che, C.-M. Cheng: New differential-algebraic attacks and reparametrization of Rainbow. ACNS 2008, LNCS vol. 5037, pp. 242 – 257. 2008.
17. A. Kipnis, A. Shamir: Cryptanalysis of the Oil and Vinegar signature scheme. CRYPTO 1998, LNCS vol. 1462, pp. 257-266. Springer, 1998.
18. P. Schwabe, B. Westerbaan: Solving Binary MQ with Grover's Algorithm. SPACE 2016, LNCS vol. 10076, pp. 303 – 322. Springer 2016.
19. Albrecht Petzoldt, Stanislav Bulygin, and Johannes Buchmann: Selecting Parameters for the Rainbow Signature Scheme – Extended Version – PQCrypto'10, pp. 21. 2010.

АНАЛІЗ МОЖЛИВОСТЕЙ ТА ОСОБЛИВОСТІ ПРОГРАМУВАННЯ ЗАДАЧ КРИПТОЛОГІЇ НА КВАНТОВОМУ КОМП'ЮТЕРІ

Останнім часом набувають обґрунтованості прогнози щодо того, що при застосуванні квантового комп'ютера для вирішення задач криптоаналізу існуючих криптоперетворень, вони, швидше за все, будуть зламані. Проте слід зауважити, що для такого застосування квантового комп'ютера, він повинен мати відповідну кубітність та відповідне розроблене математичне та програмне забезпечення. Зростання актуальності цього питання базується на успіхах у створенні робочого варіанту квантового комп'ютера [1 – 3]. Значною особливістю, що ускладнює застосування квантового комп'ютера для криптоаналізу, є те, що математичне та програмне забезпечення для квантового комп'ютера є доволі специфічним та виходить за звичні рамки, спираючись на квантові властивості. Завдяки використанню квантових властивостей, що не можуть бути використані на класичному комп'ютері, квантовий комп'ютер отримує значну перевагу над класичним у швидкодії. Так, наприклад, квантові властивості надають можливість розгляду всього регістру одночасно, замість розгляду по одному елементу за раз на класичному комп'ютері. Завдяки лише цьому досягається значна перевага в швидкодії при проведенні обчислень. Наразі для загального доступу з використанням хмарних сервісів доступними є квантові комп'ютери компанії IBM на 5 та 15 кубітів та квантового симулятора (до 32 кубітів) [6]. Ці квантові комп'ютери здатні виконувати квантові операції та реалізовувати квантові гейти. Проте слід зазначити, що більша частина квантових гейтів, можливих для реалізації, однокубітні та двохкубітні, лише декілька з них є трикубітними, в той час як робоча реалізація методу Гровера потребує гейтів, здатних на вплив на більшу кількість кубітів одночасно. Таким чином виникає необхідність розкладання багатокубітних гейтів на послідовності наявних гейтів. Враховуючи вказане було вироблено три схеми застосування методу Гровера на квантовому комп'ютері для квантового регістру з чотирьох кубітів для отримання квантового регістру.

Метою цієї доповіді є обґрунтування підходів до аналізу можливостей та вивчення особливостей програмування задач криптоаналізу на квантових комп'ютерах, а також оцінки сучасного стану можливостей його реалізації на однокубітних, двохкубітних та трикубітному гейтах.

Особливості та можливості квантового комп'ютера.

Відмінності між квантовими та класичними комп'ютерами в самих принципах роботи. Квантові комп'ютери використовують специфічну квантову інформатику, що базується на таких властивостях квантових об'єктів, як [1-3]: здатність квантової частки приймати декілька станів одночасно (завдяки квантовій суперпозиції станів); здатність систем з декількох квантових часток перебувати в переплутаних станах та, внаслідок цього, нелокальність; вплив процесу вимірювання на стан об'єкта, що може призвести навіть до знищення; практична неможливість клонування станів квантових часток. Ці властивості базуються на властивостях квантової фізики, що покладена в основу квантової інформатики.

На основі квантових властивостей квантових об'єктів розроблено специфічну квантову математику, яку покладено в основу квантових алгоритмів криптоаналізу. Основними є [4]:

- алгоритм Шора для здійснення факторизації надвеликих цілих чисел;
- алгоритми вирішення задач дискретного логарифму в скінченному полі;
- алгоритми дискретного логарифмування в групі точок еліптичних кривих;
- алгоритм пошуку в несортованій базі (метод Гровера);
- алгоритми криптоаналізу перетворень в кільцях поліномів та фактор-кільцях тощо.

Ці алгоритми розроблено для вирішення задач, що є неможливими або нерентабельно складними щодо необхідного обчислювального ресурсу для вирішення за допомогою класичних комп'ютерів [1 – 4]. Квантові алгоритми мають ймовірнісну природу, що визначає

проблемність вирішення задач криптоаналізу за допомогою квантових алгоритмів, як необхідність отримання результату з необхідною ймовірністю при вимірюванні стану квантового регістру. Як теоретично, так і практично підтверджено, застосування квантових алгоритмів на класичному комп'ютері не тільки не дає переваги, а є дуже не вигідним з точки зору швидкодії [5]. Так, наприклад, реалізація методу Гровера на класичному комп'ютері є не вигідною через те, що сам алгоритм передбачає для отримання потрібного результату при вимірюванні стану квантового регістру, багаторазового повторення ітерації Гровера. Тоді як на квантовому комп'ютері повтори покращують результат, а квантові властивості нівелюють затрати на повтори. В той час як на класичному комп'ютері ці повтори не є потрібними, а лише зайвими. Щодо властивостей, що нівелюють для квантового комп'ютера проведення повторів, то вони пояснюються тим, що квантовий комп'ютер дозволяє переглядати весь результат в регістрі всього однією операцією, в той час, як на класичному комп'ютері перегляд регістру здійснюється по одному елементу за одну операцію.

Необхідно також зазначити, що поява квантового комп'ютера, регістр котрого матиме для здійснення квантового криптоаналізу достатню кількість кубітів, є необхідною умовою зламу існуючих асиметричних криптоалгоритмів з обмеженими розмірами системних параметрів. Достатньою умовою є наявність також відповідного математичного та програмного забезпечень, а також ще й реалізації на квантовому комп'ютері безпосередньо алгоритмів, з використанням котрих можна провести криптоаналіз.

Аналіз можливостей та наявності забезпечень для вирішення задач криптоаналізу.

Таким чином, завдяки сучасним успіхам в створенні квантового комп'ютера, існує можливість доступу до програмування квантового комп'ютера за допомогою хмарних сервісів. Так наразі для загального доступу з використанням хмарних сервісів доступними є квантові комп'ютери компанії IBM на 1, 5 та 15 кубітів [1, 6]. Вони виконують квантові операції та можуть реалізовувати квантові гейти. Також можна скористатися квантовим симулятором (до 32 кубітів) [1, 6]. Наш практичний аналіз показав, що загальнодоступними для використання є однокубітні та двохкубітні, та декілька (два) трикубітних гейти. Але робочі реалізації, наприклад, методу Гровера, потребує наявності квантових гейтів, що діяли б на більшу кількість кубітів одночасно. Тому багатокубітні гейти доводиться розкладати на послідовності наявних гейтів. Наш пошук показав [1, 6], що серед доступних для загального доступу квантових комп'ютерів наявні: *ibmq_16_melbourne* (15 кубітів), *ibmq_london* (5 кубітів), *ibmq_burlington* (5 кубітів), *ibmq_essex* (5 кубітів), *ibmq_ourense* (5 кубітів), *ibmq_vigo* (5 кубітів), *ibmq_5_yorktown-ibmqx2* (5 кубітів), *ibmq_armonk* (1 кубіт). Квантовий симулятор *ibmq_qasm_simulator* може використовуватись для реалізації алгоритмів, що передбачають використання регістрів з довжиною до 32 кубітів.

Особливість квантового програмування для методу Гровера.

Одним з основних квантових методів, що є необхідними для вирішення задач криптології є метод Гровера. Розглянемо його детальніше.

Алгоритм Гровера будується з використанням методу Гровера, він є квантовим алгоритмом, що призначений для проведення вичерпного пошуку унікального елемента в несортованій базі даних, що містить $N = 2^n$ елементів, де n позначає довжину задіяного для представлення пошукового простору квантового регістру (кількість кубітів в ньому), а N є розміром пошукового простору [2, 5]. Особливість алгоритму Гровера полягає в тому, що, завдяки квантовим властивостям та використанню функції «чорної скриньки» (у вигляді квантового оракула), він потребує лише $O(\sqrt{N})$ групових операцій замість $O(N)$ у класичних алгоритмів. Квадратичне прискорення у порівнянні з класичними алгоритмами досягається завдяки використанню квантових властивостей, таких як квантова суперпозиція станів. Хоча інші квантові алгоритми при порівнянні з класичними аналогами можуть забезпечити експоненційне прискорення, а алгоритм Гровера може забезпечити лише квадратичне прискорення, слід зауважити, що навіть таке прискорення є дуже значним та його значущість збільшується зі зростанням N . Метод Гровера, як і більшість квантових

методів, є ймовірнісним, тобто правильна відповідь може бути виміряна з квантового регістру з певною ймовірністю, яка не повинна перевищувати 1. Також слід зауважити, що при виконанні більшого числа ітерацій, ніж потрібно, ймовірність виміру правильного результату зменшується, тому це потрібно відповідним чином відслідковувати [5]. Метод Гровера має ряд можливостей для застосування, одним з котрих є реалізація його як алгоритму криптоаналізу симетричних перетворень, функцій гешування, асиметричного шифру в кільці поліномів тощо у зв'язку з його можливим узагальненим використанням [1, 5]. Для криптоаналізу симетричних блокових перетворень метод можна звести до алгоритму пошуку сеансового чи довгострокового ключа тощо. У випадку функцій гешування метод можна застосувати для пошуку колізій тощо. Метод Гровера має значні потенційні можливості, котрі беруться в розрахунок з огляду на сучасний стан розробки квантового комп'ютера.

Сутність та застосування методу Гровера.

Для розуміння методу Гровера необхідно визначити квантову суперпозицію станів [1, 5]. Нехай $|\psi\rangle$ – суперпозиція всіх станів (згідно нотації Дірака):

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle.$$

З урахуванням цього, алгоритм приймає такий вигляд:

1) Встановлення системи в стан суперпозиції $|\psi\rangle$.

2) Виконання «ітерації Гровера» (або ж G) $\frac{\pi}{4}\sqrt{N}$ разів, де $N = 2^n$ та N становить

розмір пошукового простору, а n – розмір квантового регістру, що використовується для представлення пошукового простору. При цьому G включає в себе 2 етапи:

2.1) Застосування квантового оракула (O).

2.2) Застосування оператора дифузії, що здійснює «інверсію щодо середнього» та має вигляд $2|0\rangle\langle 0| - I$.

3) Виконання класичних вимірювань регістру для отримання результату роботи алгоритму, що з ймовірністю близькою до 1 буде вірним.

Практичний приклад

З метою демонстрації дії методу Гровера на практиці розглянемо приклад використання алгоритму пошуку несортованою базою даних з невеликим розміром пошукового простору, як було зроблено в [5]. Приклад [5]. Припустимо, що система може приймати $N = 72057594037927936 = 2^{56}$ станів, що означає, що база для пошуку складається з 72057594037927936 елементів. Також припустимо, що стан системи, котрий ми хочемо отримати в результаті пошуку, x_0 , має індекс 234.

1) Для описання системи необхідно $n=56$ кубітів. Згідно з алгоритмом Гровера ініціалізуємо квантовий регістр, що складатиметься з $n=56$ кубітів, що є необхідною умовою для представлення пошукового простору, що має розмір $N = 2^{56}$, встановивши регістр у початковий стан, що має наступний вигляд:

$$|\psi_0\rangle = |000\dots 000\rangle,$$

де кількість нулів дорівнює 56.

2) Проведемо перетворення Адамара, що дозволяє встановити систему в стан квантової суперпозиції, що робить значення амплітуди, що пов'язана з кожним станом, таким, щоб ймовірність перебування в кожному з 2^{56} можливих станів була рівною. Цей крок матиме наступний вигляд:

$$|\psi\rangle = H^{\otimes 56} |000\dots 000\rangle = (H|0\rangle)^{\otimes 56} = \frac{1}{268435456} \sum_{i=0}^{2^{56}} |i\rangle$$

Таким чином ми маємо квантовий регістр встановлений в стан суперпозиції, що геометрично можна представити так, як наведено на рис. 1.

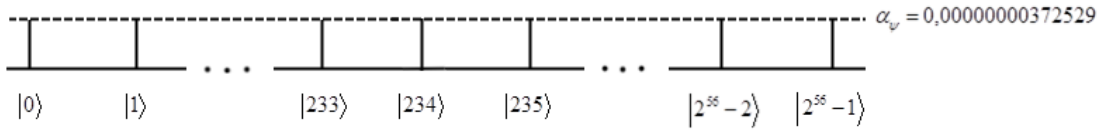


Рис. 1 – Геометричне представлення регістру з 256 кубітів в стані суперпозиції

3) Визначаємо кількість потрібних ітерацій G :

$$\frac{\pi}{4} \sqrt{2^n} = \frac{\pi}{4} \sqrt{2^{56}} = \frac{2^{28} \pi}{4} \approx 210828714,133156$$

Далі для використання в розрахунках округлимо число ітерацій до 210828714 у зв'язку з округленням вниз.

4) Після цього визначимо $|u\rangle$:

$$|u\rangle = \frac{1}{\sqrt{2^{56}-1}} \sum_{\substack{i=0 \\ i \neq 301}}^{2^{56}-1} |i\rangle = \frac{|0\rangle + |1\rangle + \dots + |2^{56}-2\rangle + |2^{56}-1\rangle}{\sqrt{2^{56}-1}}.$$

Також маємо, що:

$$|\psi\rangle = \frac{\sqrt{2^{56}-1}}{2^{28}} |u\rangle + \frac{1}{2^{28}} |234\rangle.$$

5) Далі, зі здійснення звернення до оракула, починається перша ітерація. Після застосування оракула маємо:

$$|\psi_1\rangle = |\psi\rangle - \frac{1}{2 \cdot 2^{28}} |234\rangle = |\psi\rangle - \frac{1}{536870912} |234\rangle.$$

Стан даного регістру після застосування оракула під час першої ітерації Гровера має геометричне відображення, що наведено на рис. 2.

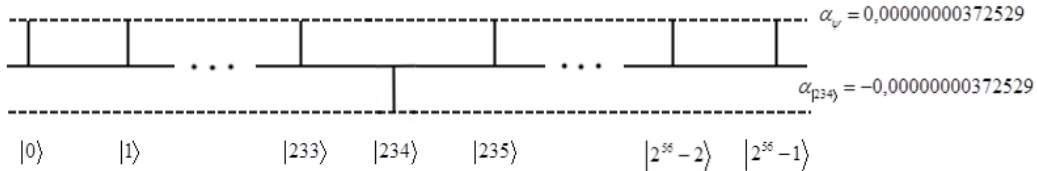


Рис. 2 – Геометричне відображення стану регістру після застосування оракула під час першої ітерації G

Далі відбувається виконання оператора дифузії, в результаті чого отримуємо:

$$|\psi_2\rangle = (2|\psi\rangle\langle\psi| - I)|\psi_1\rangle = 0,999999999999999861|\psi\rangle + 0,0000000018626|234\rangle.$$

Геометричне відображення стану регістру після першої ітерації зображено на рис. 3.

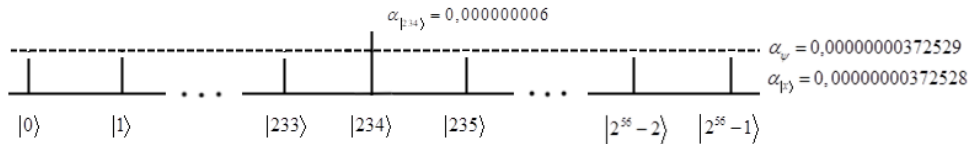


Рис. 3 – Геометричне представлення стану квантового регістру після проведення першої ітерації G

Далі аналогічним чином проводиться ще 210828713 ітерацій.

Під час проведення останньої, 210828714-й ітерації маємо в результаті застосування оракула:

$$|\psi_{421657427}\rangle = 0,000000000000003|\psi\rangle - 0,9999999999999841|234\rangle.$$

Стан даного регістру після застосування оракула під час останньої ітерації Гровера має геометричне відображення, що наведено на рис. 4.

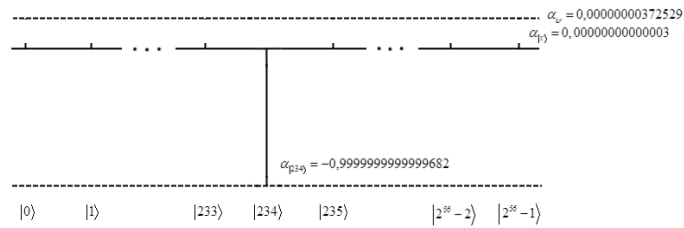


Рис. 4 – Геометричне відображення стану реєстру після застосування оракула під час останньої ітерації G

Після застосування оператора дифузії під час останньої ітерації маємо:

$$|\psi_{421657428}\rangle = (2|\psi\rangle\langle\psi| - I)|\psi_{421657427}\rangle = -0,000000000000001|\psi\rangle + 0,9999999999999841|234\rangle.$$

Геометричне представлення результатів останньої ітерації наведено на рис. 5.

Ймовірність отримання потрібного елементу в результаті вимірювання реєстру після проведення дванадцяти ітерацій становить:

$$P \approx |0,9999999999999841|^2 \approx 0,9999999999999682 \approx 99,99999999999682\%.$$

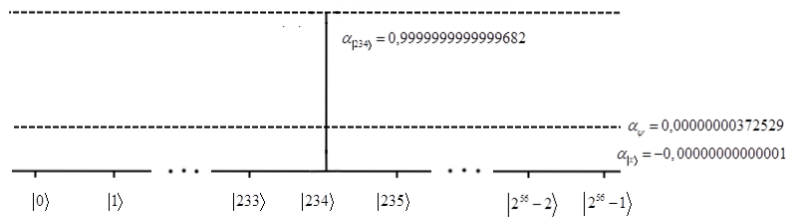


Рис. 5 – Геометричне представлення стану квантового реєстру після проведення останньої ітерації G

Таким чином, на цьому прикладі, враховуючи попередні, можна побачити, що зі зростанням N похибка дійсно стає незначною. Також слід зазначити, що приклад було розраховано з використанням програмної моделі проведення пошуку методом Гровера, що була модернізована на швидкодію. В загальному вигляді програмна модель, використана для розрахунків, відповідає загальній програмній моделі методу Гровера, але відрізняється тим, що оракул було спрощено до елементарної функції пошуку, що також проводилася повністю лише в частині відповідальній за ініціалізацію. Така побудова моделі дозволила провести розрахунки без вирішення складної задачі пошуку, але зі збереженням достовірності результатів розрахунків на рівні, що відповідає рівню достовірності результатів програмної моделі, що проводить виконання складної задачі пошуку.

5. *Схеми застосування методу Гровера на квантовому комп'ютері для квантових реєстрів з використанням хмарних сервісів.* Наразі для загального доступу з використанням хмарних сервісів доступними є квантові комп'ютери компанії IBM на 5 та 15 кубітів та квантового симулятора (до 32 кубітів) [6]. Вони виконують квантові операції та можуть реалізовувати квантові гейти. Слід відмітити, що ці гейти однокубітні та двохкубітні, а один з них трикубітний. Робоча реалізація методу Гровера в свою чергу потребує наявності квантових гейтів, що діяли б на більшу кількість кубітів одночасно. Тому багатокубітні гейти доводиться розкладати на послідовності гейтів, що є в наявності серед універсальних.

Враховуючи все наведене було вироблено три схеми застосування методу Гровера на квантовому комп'ютері для квантового реєстру з чотирьох кубітів для отримання результату «0», що може бути представлено рядком бітів $|0000\rangle$, та три схеми для отримання результату 4, що може бути представлено рядком бітів $|0100\rangle$. Схеми відрізняються кількістю застосування ітерацій Гровера. Так в перших схемах застосовується одна ітерація Гровера, в других – дві ітерації, в третіх – три ітерації. Ці схеми було випробувано на доступних для загального доступу тестових квантових комп'ютерах компанії IBM та доступному через той же сервіс квантовому симуляторі [6]. Серед квантових комп'ютерів, що використані в дослідженні, були: *ibmq_16_melbourne*, *ibmqx2* (він же *ibmq_5_yorktown-ibmqx2*), *ibmq_burlington*. Квантовий симулятор *ibmq_qasm_simulator* може розраховувати схеми,

що передбачає використання до 32 кубітів. Як вже було зазначено, особливості реалізації методу Гровера для квантового регістру, що складається з чотирьох кубітів на квантовому комп'ютері включають в себе необхідність застосування 3-кубітних квантових гейтів. В той же час інструментарій для взаємодії з доступними квантовими комп'ютерами не включає в себе квантові гейти, що оперують над потрібною кількістю кубітів. Потрібні квантові гейти можна замінити сукупностями наявних в інструментарії квантових гейтів, що дають той самий ефект.

Результати виконаних випробувань можуть вказувати як на недосконалість методів, використаних для представлення багатокубітних гейтів у вигляді сукупності одно- та двокубітних гейтів, так і на недосконалість розроблених квантових комп'ютерів, що підлягає перевірці в майбутніх дослідженнях. Результати застосування методу Гровера з однією ітерацією для отримання $|0000\rangle$ показали значні розбіжності між реальними результатами та отриманими за допомогою квантового симулятора. Так, симулятор вказував на те, що ймовірність отримання $|0000\rangle$ становить 46,875%, в той час як при проведенні реальних вимірювань цей результат було отримано лише 6,152% разів на *ibmq_burlington*, 7,52% - на *ibmqx2* та 8,789% – на *ibmq_16_melbourne* квантових комп'ютерах. Результати застосування методу Гровера з двома ітераціями для отримання $|0000\rangle$ показали ще більші розбіжності між очікуваними та реальними результатами. Так, на симуляторі ймовірність отримання $|0000\rangle$ становила 91,211%, в той час як насправді було отримано лише 6,543% на *ibmq_burlington*, 8,398% на *ibmqx2* та 10,156% на *ibmq_16_melbourne* квантових комп'ютерах. Результати застосування методу Гровера з трьома ітераціями (що є остаточною кількістю ітерацій для регістру цього розміру) для отримання $|0000\rangle$ підтвердили розбіжності, отримані на попередньому кроці. Так, симулятор спрогнозував ймовірність отримання $|0000\rangle$ в 96,387%, в той час як на реальних квантових комп'ютерах було отримано потрібний результат значно меншу кількість разів: 7,227% – на *ibmq_burlington*, 8,301% – на *ibmqx2*, 9,961% на *ibmq_16_melbourne* квантовому комп'ютері.

Результати застосування методу Гровера з однією ітерацією для отримання $|0100\rangle$ показали значні розбіжності між реальними результатами та отриманими за допомогою квантового симулятора. Так, симулятор вказував на те, що ймовірність отримання $|0100\rangle$ становить 46,387%, в той час як при проведенні реальних вимірювань цей результат було отримано лише 5,469% разів на *ibmq_burlington*, 10,547% – на *ibmqx2* та 6,506% – на *ibmq_16_melbourne* квантових комп'ютерах. Результати застосування методу Гровера з двома ітераціями для отримання $|0100\rangle$ показали ще більші розбіжності між очікуваними та реальними результатами. Так, на симуляторі ймовірність отримання $|0100\rangle$ становила 90,259%, в той час як насправді було отримано лише 6,006% на *ibmq_burlington*, 6,982% на *ibmqx2* та 6,897% на *ibmq_16_melbourne* квантових комп'ютерах. Результати застосування методу Гровера з трьома ітераціями для отримання $|0100\rangle$ підтвердили розбіжності, отримані на попередньому кроці. Так, симулятор спрогнозував ймовірність отримання $|0100\rangle$ в 96,436%, в той час як на реальних квантових комп'ютерах було отримано потрібний результат значно меншу кількість разів: 6,299% – на Бурлінгтонському, 6,152% – на Йорктаунському, 7,837% на Мельбурнському квантовому комп'ютері.

Висновки. 1. Подальший розвиток вимагає удосконалення представлення багатокубітних гейтів шляхом використання одно- та двокубітних гейтів, а також вдосконалення оснастки для роботи з квантовими комп'ютерами та розробки багатокубітних гейтів та впровадження їх у діючі зразки квантових комп'ютерів.

2. Хоча квантовий симулятор вказує на те, що схеми повинні надавати правильний результат із ймовірністю близькою до максимальної, результати реальних експериментів не є навіть близько такими вдалими.

3. Реалізація методу Гровера на класичному комп'ютері є не вигідною через те, що сам алгоритм передбачає для отримання потрібного результату при вимірюванні стану квантового регістру, багаторазове повторення ітерації Гровера. Тоді як на квантовому комп'ютері повтори покращують результат, а квантові властивості нівелюють затрати на повтори. В той час як на класичному комп'ютері ці повтори не є потрібними, а лише зайвими.

4. Щодо властивостей, що нівелюють для квантового комп'ютера проведення повторів, то вони пояснюються тим, що квантовий комп'ютер дозволяє переглядати весь результат в регістрі всього однією операцією, в той час, як на класичному комп'ютері перегляд регістру здійснюється по одному елементу за одну операцію.

5. Необхідно також зазначити, що поява квантового комп'ютера, регістр якого матиме для здійснення квантового криптоаналізу достатню кількість кубітів, є суттєво необхідною умовою зламу існуючих асиметричних криптоалгоритмів з обмеженими розмірами системних параметрів.

6. Достатність умови в тому, що окрім власне квантового комп'ютера, необхідним ще є наявність відповідного математичного та програмного забезпечень, а також ще й реалізації на квантовому комп'ютері безпосередньо алгоритмів, з використанням яких можна провести криптоаналіз.

7. Можна стверджувати, що створення квантового комп'ютера призведе до появи значної загрози для сучасних криптографічних систем з боку вже розроблених квантових алгоритмів, таких як алгоритми Гровера та Шора тощо.

8. Питання програмування задач взагалі криптології, особливо криптоаналізу, з орієнтацією на квантовий комп'ютер, стає все більш актуальним. Такі можливості з'явилися завдяки успіхам у справі створення робочого варіанту екземпляру квантового комп'ютера.

9. Як математичне, так і програмне забезпечення квантового комп'ютера є суттєво специфічними і не вкладаються в наші звичні рамки. В той же час, необхідність вирішення задач криптоаналізу на квантовому комп'ютері пояснюється його суттєвою перевагою перед класичним у швидкодії.

10. З отриманих результатів можна зробити висновок, що нинішні квантові комп'ютери ще не здатні на повноцінне контрольоване відтворення всіх квантових властивостей. Хоча можливо з більшою кількістю кубітів метод Гровера і даватиме кращий результат, що буде перевірено подальшими дослідженнями.

11. Причини таких результатів та можливість отримання кращих результатів підлягають подальшим дослідженням.

ЛІТЕРАТУРА

1. Квантовые компьютеры. [Електронний ресурс]. – Режим доступу: <http://www.nkj.ru/archive/articles/5309/>.

2. Lov K. Grover, A fast quantum mechanical algorithm for database search, 1996. – Режим доступу: <https://arxiv.org/pdf/quant-ph/9605043.pdf>.

3. Feynman, R. P. Quantum mechanical computers / R. P. Feynman // Opt. News – 1985. – February.11. – pp.. 11 – 39.

4. Горбенко, І. Д. Прикладна криптологія : монографія / І. Д. Горбенко, Ю. І. Горбенко; ХНУРЕ. – Х.: Форт, 2012. – 868 с.

5. Сутність та особливості реалізації методу Гровера на класичному комп'ютері для симетричного криптоаналізу / Ю. І. Горбенко, Є. Ю. Каптьол // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. – 2018. Вип. 195. – С. 89 – 100.

6. IBM Quantum Experience Dashboard. [Електронний ресурс] – Режим доступу: <https://quantum-computing.ibm.com/>.

СУЧАСНІ СИСТЕМИ УПРАВЛІННЯ БПЛА ТА ТРАЄКТОРНЕ УПРАВЛІННЯ

Вступ. Застосування БПЛА відкриває можливість оперативного і недорогого способу виконання ряду специфічних завдань:

- розвідка важкодоступних районів, в яких отримання інформації звичайними засобами, включаючи авіарозвідку, ускладнене або ж наражає на небезпеку здоров'я і навіть життя людей;
- періодичне спостереження за заданими районами, де потрібен нагляд за місцевістю і об'єктами на ній з повітря, в тому числі і з високоточним визначенням координат об'єктів (моніторинг стану енергетичних комунікацій, газо- і нафтопроводів, авіабезпека та ін.);
- цифрове фотографування для використання в геодезичних роботах і у випадках надзвичайних ситуацій;
- доставка вантажів і виконання специфічних видів робіт (обробка хімікатами сільськогосподарських посівів, участь в рятувальних операціях) та ін.

Комплекс управління сучасних міні, мікро-БПЛА складається з бортової системи автоматичного управління (САУ) або автопілота і наземного обладнання - наземної станції управління (НСУ), до складу яких входять різні датчики і мікроконтролери зі спеціалізованим програмним забезпеченням, апаратура контролю, управління і зв'язку, електроживлення. САУ БПЛА – лише частина складного багатофункціонального комплексу, яка реалізує часткові функції всього комплексу і дозволяє виконувати перераховані вище завдання.

САУ сучасних міні, мікро-БПЛА ґрунтується на мікромеханічних датчиках тиску, кутових швидкостей і прискорень (MEMS-сенсорах), а також мікромагнетометрах (магнітних компасах) і супутникових радіонавігаційних приймачах (GNSS-приймачах) [3, 4]. Такі сенсори дозволяють проектувати мініатюрні системи вимірювання параметрів руху (безплатформенні інерціальні навігаційні системи - БІНС) і системи управління ЛА від літака з класичним компонуванням до оригінальних апаратів вертикального зльоту і посадки. Об'єднання БІНС і системи управління в єдиний пристрій дало поняття автопілота, як багатофункціонального пристрою з управління міні, мікро-БПЛА.

В даній статті проаналізовано можливості сучасних САУ різних фірм-виробників, а так само результати власної розробки – системи управління польотом AP-VIC, і розширенню функціональних можливостей за рахунок точного траєкторного управління. З часу публікацій про можливості систем управління [1, 2] відбулися значні доопрацювання і зміни у функціональній частині всіх систем [3 – 7], тому дана стаття доповнює опис можливостей сучасних систем управління.

1. Порівняльний аналіз сучасних систем управління польотом

Розглянемо особливості систем управління БПЛА, які доступні на ринку авіоніки, а також можливості власної розробки „AP-VIC”.

Автопілот серії MP2x28 фірми Micropilot (Канада)

Фірма Micropilot є одним зі світових лідерів з виробництва автопілотів для БПЛА (понад 850 клієнтів в 70 країнах світу). Випускає серію автопілотів MP2x28 призначених для використання на міні-БПЛА літакового, вертолітного, а також мультироторного типів. Вартість автопілотів серії MP2x28 для БПЛА літакової схеми коливається від \$ 1700 до \$ 8000 USD. Розміри автопілота MP2x28 в базовому одноплатному безкорпусному виконанні становить 100x40x15 мм при вазі всього 24 грами [9].

Автопілот „Vector” фірми UAV Navigation (Іспанія)

Компанією UAV Navigation розроблений і з 2014 року вироблявся професійний автопілот „Vector”, який прийшов на зміну „AP04”, що випускався з 2004 по 2014 рр. Він може використовуватися на міні-БПЛА літакового, вертолітного та мультироторного типу

[10]. АП може використовуватися як на БПЛА, оснащених двигунами внутрішнього згорання, так і електричними, і реактивними двигунами. „Vector” – це повністю інтегрований автопілот з можливістю ручного управління БПЛА, вбудованим радіоканалом і можливістю управління корисним навантаженням. Даний автопілот забезпечує автоматичний зліт, політ по заданому маршруту і автоматичне приземлення. Вбудований радіоканал дозволяє передавати дані на відстань до 100 км. Механізм ручного управління дозволяє оператору на землі повністю управляти БПЛА за допомогою стандартного джойстика, або стандартної апаратури управління, призначеної для авіамоделей. АП «Vector» містить дублюючий мікропроцесор, який забезпечує високий рівень безпеки та відмовостійкості, самотестування датчиків. Фактично „Vector” може бути єдиною апаратурою управління на борту для більшості БПЛА. Автопілот дозволяє управляти шістнадцятьма виконавчими пристроями або іншою периферією. Він забезпечує автоматичний політ за маршрутом у вигляді контрольних точок, які мають три виміри (широта, довгота, висота).

Орієнтовна вартість автопілота „Vector” становить від 6000 євро.

Автопілот серії Piccolo фірми Cloud Cap Technology, Inc. (США)

Компанія Cloud Cap Technology – також є однією з провідних компаній в області технологій БПЛА. Сімейство автопілотів Piccolo включає кілька модифікацій і всі вони розроблені для управління БПЛА літакового, вертолітного й мультироторного типів. «Piccolo II» є повнофункціональним автопілотом з інтегрованою БІНС, GPS-приймачем, системою повітряних сигналів і радіомодемом в полегшеному карбоновому корпусі. Як і АП «Vector» може бути єдиною апаратурою управління на борту БПЛА. Недолік – відносно великі розміри: 142x46x63 мм і маса (200 г), що ускладнює його використання на мікро-БПЛА. Більш придатними для використання на міні, мікро-БПЛА є модифікації „Piccolo SL» і „Piccolo Nano” [11].

Інерціальні датчики калібровані для робочих температур від -40°C до + 80°C.

„Piccolo Nano” оптимальний за розмірами автопілот для невеликих електричних БПЛА і являє собою модульний автопілот в безкорпусному виконанні з розмірами модуля – 77x46x11 мм. У порівнянні зі «старшими» братами сімейства має дещо більш вузький температурний діапазон калібрування датчиків (-30°C ... + 80°C) і трохи ширший діапазон живлячих напруг (+ 6В ... + 30В).

Базова ціна автопілотів Piccolo не менше \$ 8000 USD. Обмеження автопілота – необхідність авторизації клієнта (отримання дозволу) при експорті автопілота за межі території США.

Автопілот „GNC1000» фірми Moog Crossbow's (США)

Комплект автопілота „GNC1000” для середніх БПЛА виробляється фірмою Moog Crossbow's [8,12]. Містить досить продуктивний процесор MPC5674F з тактовою частотою 264 МГц і широкий набір мережевих інтерфейсів (RS-485, CAN, Ethernet). Потужні обчислювальні можливості гарантують виконання в реальному часі алгоритмів розширеної калмановської фільтрації і реалізацію алгоритмів управління.

Конструктивне виконання відповідає рівню захисту від зовнішніх впливів за стандартом IP67, також відповідає військовим стандартам США (MIL-STD-461F, MIL-STD-810G, DO-160G) щодо електромагнітної сумісності, вібраційних і ударних навантажень і електростатичного захисту.

Недоліки АП – невелика кількість (шість) виходів для управління виконавчими пристроями з ШІМ-сигналом, відносно великі розміри (100x15x75 мм) і маса (близько 1,4 кг), можливо необхідний дозвіл на експорт за межі території США. Базова ціна, на жаль, також не відома.

Автопілот „Pixhawk” (PX-4) компанії 3D-robotics, Inc. (США)

Автопілот „HEX Pixhawk 2.1 CUBE ORANGE” (PX-4) це один з кращих на сьогоднішній день так званих „відкритих проєктів” (open source project), тобто проєктів з відкритим кодом і схемами [13]. Є розвитком таких відкритих проєктів як Ardupilot, APM. Розробляється, підтримується і тестується великою кількістю незалежних розробників з

усього світу. Виготовляється промислово і просувається на ринку авіоніки компанією 3D-robotics [14]. Має гарні масогабаритні показники: розміри основного модуля – 95x45x39 мм, вага – 75 г. У складі АП використовується потужний сучасний ARM-мікроконтролер з обчислювальним ядром Cortex™-M7 з тактовою частотою 400 МГц. Реалізована стандартна для такого класу АП функціональність. Орієнтовна вартість базового комплекту \$ 450- \$ 500 USD.

У відкритості проекту є і плюси і мінуси. Переваги полягають у доступності вихідних кодів, які „просунутий” споживач може адаптувати під свої завдання, а також те, що при великій кількості незалежних розробників є можливість оперативно розширювати функціональність, тестувати АП і усувати помилки (але і додавати свої). Можливість розширення проекту для інших користувачів призводить до підвищеного рівня помилок, оскільки не гарантується 100%-а тестова перевірка внесених змін. Використання такого АП передбачає ретельне тестування дослідного зразка в польоті, виявлення недоробок.

Недолік полягає ще в тому, що управління БПЛА з відкритим кодом можна „перехоплювати”, що неприпустимо при їх використанні для вирішення спеціальних завдань. Крім того, „відкриті” проекти, як правило, не забезпечують достатньої технічної підтримки користувача, який залишається «один на один» з придбаним АП або шукає „друзів” на форумах.

Можна навести й інші варіанти АП, більшість яких копіюють можливості розглянутих.

Автопілот „AP-VIC” ТОВ „БТ” (Україна)

Автопілот „AP-VIC” виконаний на основі БНС на мікромеханічних датчиках з використанням оригінальних власних алгоритмів [15 – 17]. АП побудований з міні-модульної легко розширюваної структури з використанням завадостійкого CAN-інтерфейсу зв'язку між модулями. Модульна структура його конструкції дозволяє легко розміщувати автопілот в вільних місцях не тільки міні, але і мікро-БПЛА.

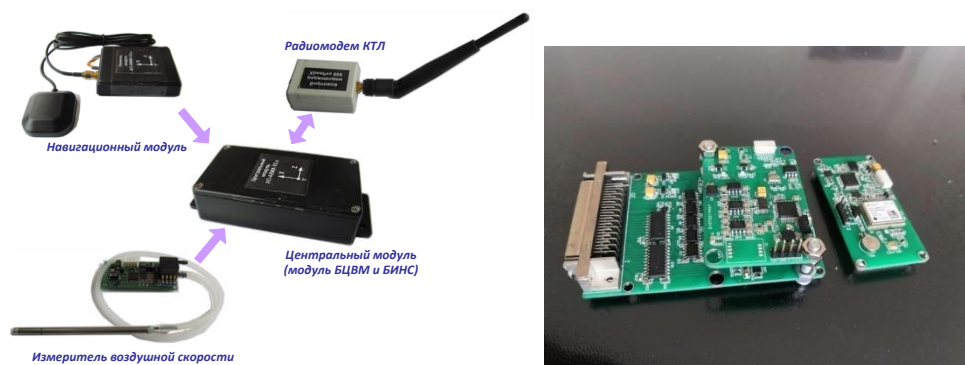


Рис.1. Автопілот „AP-VIC”

„AP-VIC” забезпечує режими автоматичного зльоту, посадки, автоматичного польоту по заданому маршруту, а також автоматичного повернення в район зльоту при перевищенні заданої дальності, при зниженні напруги живлення нижче критичного рівня для всіх типів БПЛА. Включає легко модифікуєме, під потреби замовника, програмне забезпечення нижнього та верхнього рівнів вітчизняної розробки. Підтримуються різні типи ЛА від мультироторів з 3-ма моторами, до літаково-вертолітних-гібридних ЛА. Перевагою також є постійна технічна підтримка на території України.

Крім перерахованих вище, існує велика кількість комерційних автопілотів, таких як, наприклад, автопілот серій Naza і WooKong фірми DJI [5], „Panda” фірми FeiYu Electronic Technology Co., Ltd. [6], автопілот серій 35x1, 36x1 компанії UNAV, автопілот RVOSD компанії і RangeVideo та ін.

Сучасні міні, мікро-БПЛА висувають досить жорсткі вимоги до масо-габаритних параметрів автопілотів, а також їх функціональності.

2. Порівняння можливостей АП

З аналізу характеристик АП можна зробити наступні висновки.

1) Наявні на ринку АП можна розділити на кілька класів:

– „професійні”: Vector” (UAV Navigation), „Piccolo SL” (Cloud Cap Technology), „MP2x28” (Micropilot), «GNC1000” (Moog Crossbow's), „Kestrel” (Procerus Technologies), „AP-VIC” (ТОВ«БТ”);

– „середнього” класу: „Pixhawk (PX-4)” (3D-robotics), „Naza” (DJI), „YS” (Zero UAV Intelligent Technology), „Panda” (FeiYu Electronic Technology Co).

– „аматорського” рівня: 35x1, 36x1 (UNAV), RVOSD (RangeVideo), NAZA (DJI) та ін.

Для професійних рішень потрібен дозвіл на експорт з країни виробника, вони виконані з високим рівнем захисту і мають досить високу ціну.

2) Більшість АП використовують однотипні (або однакові) мікромеханічні і радіоелектронні сенсори, тому якість вирішення навігаційних завдань залежить від алгоритмів роботи АП, наявності температурної компенсації і якості калібрування датчиків.

Для мікро-міні-БПЛА важливі не тільки розміри модулів АП, а також можливість установки модуля БІНС окремо від основного модуля (у вільному місці ЛА). Такою можливістю, серед представлених АП, володіє „AP-VIC”.

Для динамічних („швидких”) БПЛА (особливо для ЛА мультироторного типу), важлива швидкість реакції АП на мінливу польотну обстановку, тому важливим параметром є частота дискретизації (частота вирішення завдання управління). Чим вона вища, тим краще, хоча для динаміки сучасних БПЛА збільшувати частоту дискретизації вище 1 кГц особливого сенсу не має. Для більшості представлених АП частота дискретизації не перевищує 200 Гц, хоча деякі АП, такі як „AP-VIC”, „MP2x28”, дозволяють встановлювати частоту дискретизації до 300 Гц.

Цей параметр безпосередньо пов'язаний з частотою оновлення даних датчиків. У „AP-VIC” вона становить 800Гц. Це дозволяє проводити додаткову обробку (наприклад, додаткову фільтрацію) сигналів датчиків.

Частота дискретизації також залежить від швидкодії мікроконтролера, який за один такт дискретизації повинен виконувати операції по обробці сигналів датчиків і формуванню сигналів управління. За продуктивністю мікроконтролера безперечним лідером є АП „HEX Pixhawk 2.1 CUBE ORANGE”, який використовує в якості мікроконтролера з процесорним ядром ARM Cortex™ -M7 з тактовою частотою 400МГц. Це дозволяє реалізувати дуже складні й вимогливі до обчислювальної потужності алгоритми обробки і управління, хоча за результатами практичного тестування завантаження центрального процесорного пристрою АП „Pixhawk” (навіть з урахуванням використання в ньому операційної системи реального часу) не перевищує 30-40%. Тобто мікроконтролер цього АП обраний з значним запасом по обчислювальній потужності (на перспективу).

Виконання польотів в складних кліматичних умовах (при температурах нижче 0°C і вище + 35°C) можливо тільки при наявності термокомпенсації сигналів датчиків. Для цього на етапі виробництва повинна проводитися температурне калібрування датчиків. Розширеним діапазоном робочих температур володіють тільки АП професійної серії, наприклад, „MP2x28” і „Kestrel”.

3) Розширення функціональних можливостей АП може здійснюватися при наявності достатньої кількості інтерфейсів для підключення зовнішніх пристроїв. Для більшості БПЛА достатнім для управління є наявність 4-5 вхідних і вихідних каналів з керуванням ШІМ-сигналами, але в деяких випадках можуть знадобитися додаткові канали управління (наприклад, для управління корисним навантаженням). Серед розглянутих, найбільшою кількістю (24 вихідних канали) володіє „MP2x28” з додатковим модулем розширення, хоча в „AP-VIC” також можливе збільшення кількості ШІМ-виходів при використанні додаткових плат розширення.

Також відмінною рисою „MP2x28” і „AP-VIC” є можливість використання додаткового каналу телеметрії – радіоканалу супутникового зв'язку і GPRS/3G-каналу, відповідно.

3. Наведення ЛА на траєкторії

Вважаємо, що наведення ЛА це завдання управління польотом по траєкторії, яка може складатися з різних видів – лінії заданого шляху (ЛЗШ) від одного проміжного пункту маршруту (ППМ) до іншого, окружності заданого радіуса або еліпса заданої орієнтації і параметрів, або інших реалізованих фігур. Часто політ по ЛЗШ застосовується для наведення ЛА в задану точку або в місцевість для баражування, для організації прольоту по маршрутним лініям при проведенні аерофотозйомки або розпилення хімічними реактивами. При такому наведенні важливо мати мінімально можливе відхилення центру мас ЛА від ЛЗШ. Таким чином, мета завдання наведення на траєкторії це мінімальна помилка відхилення ЛА від ЛЗШ. Дана помилка відхилення від ЛЗШ залежить від засобів навігації ЛА або точності поточних координат, алгоритмів наведення і зовнішнього фактора - напрямки і величини швидкості вітру. Для підвищення точності поточних координат застосовують СРНС системи з режимами роботи диференціальному (DGPS) або кінематичному (RTK GPS), що здорожує і ускладнює навігацію, але підвищує точність координат до одиниць сантиметрів. Алгоритмічний аспект наведення полягає у використанні відхилення від ЛЗШ в управлінні по курсу ЛА літакового типу, або по крену і тангажу ЛА мультироторного типу. В АП „АР-VIC” реалізований ПІД-закон управління по заданих кутах від бокового відхилення, що забезпечує астатизм системи першого порядку або нульову сталу помилку бокового відхилення ЛА від ЛЗШ. Реальні польоти різних типів ЛА з АП „АР-VIC” підтвердили ефективність алгоритмів наведення в умовах швидкості вітру до 8 м/с.

Висновок. Розглянутий склад бортового обладнання БПЛА від різних виробників дозволяє забезпечити вирішення широкого кола завдань з моніторингу місцевості і інших завдань в інтересах людини. Однак специфіка завдань щодо застосування БПЛА вимагає варіативності, як по функціональному забезпеченню, так і технічному виконанню. Одні з реалізацій вимагають варіанти легкого виконання для дешевих ЛА, інші реалізації вимагають жорстких умов за кліматичними умовами, третій варіант вимагає захищеності каналів зв'язку та ін., тому різноманітність по виконанню, за змістом представлених автопілотів розширює сфери використання БПЛА.

Розвиток чи вдосконалення засобів систем управління БПЛА вбачається не тільки в розширенні апаратних можливостей, тому що сучасні мікроконтролери „справляються” з різноманітним програмним забезпеченням, а в розширенні функціональних можливостей, в тому числі функцій точного наведення і надійності БПЛА.

ЛІТЕРАТУРА

1. Jung Soon Jang and D. Liccardo, „Automation of small UAVs using a low cost MEMS sensor and embedded computing platform,” in 25th Digital Avionics Systems Conference, 2006 IEEE/AIAA, October 2006, pp. 1 – 9.
2. Jose A. Rios, Elecia White, “Fusion filter algorithm enhancements for a MEMS GPS/IMU” Crossbow Technology, Inc., Режим доступа к электронному документу: http://www.moogrossbow.com/Literature/Application_Notes_Papers/Fusion_Filter_Algorithm_Enhancements_for_a_MEMS_GPS-IMU.pdf
3. Кортунов В.И., Мазуренко О.В., Ватик Махаммед Али Хусейн, „Средства управления мини и микро-БПЛА” // Радиоэлектронні і комп’ютерні системи. – Х.: Нац. аерокосмічний ун-т „Харк. авіац. ін-т”, 2016. – № 1(75) – С. 45 – 55.
4. V.I. Kortunov, W.Mohammed, A.Gorbenko, O. Mazurenko, „Review and Comparative Analysis of Mini- and Micro-UAV Autopilots” // 2015 IEEE 3rd International Conference „Actual problem of Unmanned Aerial Vehicles Developments (APUAVD)” – С. 284 – 299.
5. M.Furkan Bahat, „Autopilot”, Anadolu University, 2013, December 7, pp.1-3, Режим доступа к электронному документу: <http://www.suasanadolu.com/autopilot/>
6. HaiYang Chao, YongCan Cao, and YangQuan Chen, „Autopilots for Small Unmanned Aerial Vehicles: A Survey”, International Journal of Control, Automation, and Systems, 2010, 8(1),

- pp.36 – 44, Режим доступа к электронному документу: <http://www.springer.com/12555DOI10.1007/s12555-010-0105-z>
7. Руснак І.С. Безпілотна авіація у сфері цивільного захисту України. Стан і перспективи розробки та застосування / І.С. Руснак, В.В. Хижняк, В.І. Ємець // Наука і оборона. – 2014. – №2 – С. 34 – 39.
8. Inertial Sensors, IMU and AHRS, CrossBow Company, Aerospace and Defense Systems, Режим доступа к электронному документу: <http://www.moog-crossbow.com/products/inertial-products>.
9. MP2x28 Series Autopilots, MicroPilot Company, Режим доступа к электронному документу: <http://www.micropilot.com/products-mp2028-autopilots.htm>.
10. VECTOR. Autonomous Flight Control Unit, UAV Navigation, Режим доступа к электронному документу: <http://uavnavigation.com/products/uav-autopilot-vector>.
11. Piccolo Autopilots, CloudCap Technology, Режим доступа к электронному документу: <http://www.cloudcaptech.com/products/auto-pilots>.
12. Flight Management Systems - Vehicle Management Computers, CrossBow Company, Aerospace and Defense Systems, Режим доступа к электронному документу: <http://www.moog-crossbow.com/products/flight-management-systems-vehicle-management-computers/products-gnc1000>.
13. Pixhawk Autopilot, Pixhawk Community, Режим доступа к электронному документу: <https://pixhawk.org/modules/pixhawk>.
14. 3DR Pixhawk Autopilot, 3D3D Robotics, Inc, Режим доступа к электронному документу: <https://store.3drobotics.com/products/3dr-pixhawk>.
15. V.I. Kortunov Integrated MimiINS Based on MEMS Sensor for UAV Control / Kortunov V.I., Dybska I.Yu., Proskura G.A., Kravchuk A.S. // IEEE A&E System magazine – 2009. – January. – Pp. 41 – 43.
16. Картунов В.И. Экспериментальное исследование точности коррекции интегрированной миниатюрной БИНС / В.И. Картунов, Г.А. Проскура, А.С. Кравчук // Електроніка та системи управління. – 2008. – №1(15) – С. 26 – 33.
17. Картунов В.И. Наблюдаемость инструментальных погрешностей интегрированной бесплатформенной инерциальной навигационной системы и методика их оценивания / Г.А. Проскура, В.И. Картунов // Авиационно-космическая техника и технология. – 2008. – № – С.7 – 12 .

КЛЮЧОВА АТАКА ВІДНОВЛЕННЯ CIRCULANT UOV/RAINBOW

Багатовимірна криптосистема з відкритим ключем (МРКС) – це криптосистема відкритого ключа, відкритий ключ якої є набором багатовимірних квадратних форм над обмеженим полем. Очікувалося, що МРКС будуть постквантовою криптографією, оскільки проблема вирішення системи багатоваріантних нелінійних поліномів є NP-Hard [1, 2]. Неврівноважена схема підпису олії та оцту (UOV) [3,4] та Rainbow [5] можна вважати двома найуспішнішими схемами багатовимірного підпису, оскільки покоління підписів ефективні, а безпека від відомих атак достатня за відповідним параметром виділення. Насправді кілька МРКС, поданих до проекту постквантової криптографії криптографії NIST [6], базуються на UOV та Rainbow. Нещодавно Пенг і Тан запропонували нові варіанти UOV та Rainbow під назвою Circulant UOV [7] та Circulant Rainbow [8] відповідно. У цих варіантах коефіцієнти квадратних форм на центральних картах вибираються такими, що циркуляційні матриці з'являються в процесі генерації підпису. Оскільки інвертування матриці циркуляції швидше, ніж інвертування випадкової матриці, генерація сигнатур Circulant UOV/Rainbow відбувається швидше, ніж оригінальна схема. Однак такі „циркуляційні” структури критично послаблюють безпеку. У цьому докладі ми ретельно вивчаємо структури Circulant UOV та Circulant Rainbow і робимо висновок, що еквівалентні секретні ключі можуть бути вилучені атакою Кіпніса-Шаміра [4,9] за багаточлен.

2. UOV

Спочатку опишемо незбалансовану схему підпису олії та оцту (UOV) [3,4] та атаку Кіпніса-Шаміра на UOV [4,9]. Нехай $n, o, v \geq 1$ - цілі числа з $v \geq o$, $n = o + v$, q - сила простих, а F_q – кінцеве поле порядку q . Визначте квадратичну карту $G: F_q^n \rightarrow F_q^o$, $x = {}^t(x_1, \dots, x_n) \rightarrow G(x) = {}^t(g_1(x), \dots, g_o(x))$ по $g_l(x) = \sum_{1 \leq i \leq o} x_i$ (лінійна форма $x_{o+1}, \dots, x_n$) + (квадратична форма $x_{o+1}, \dots, x_n$) ($1 \leq l \leq o$), де коефіцієнти в правій частині - це елементи F_q . Незбалансована схема підпису олії та оцту (UOV) будується наступним чином.

Секретний ключ. Оборотна афінна карта $S: F_q^n \rightarrow F_q^n$ та квадратична карта G , визначена вище. Публічний ключ. Квадратична карта $F: F_q^n \rightarrow F_q^o$.

Генерація підписів. Для повідомлення $m = {}^t(m_1, \dots, m_o) \in F_q^o$, який потрібно підписати, виберіть випадково $u_1, \dots, u_v \in F_q$ і знайдіть $(y_1, \dots, y_o) \in F_q^o$ з

$$g_1(y_1, \dots, y_o, u_1, \dots, u_v) = m_1, \quad (1)$$

$$\dots, g_o(y_1, \dots, y_o, u_1, \dots, u_v) = m_o$$

Підпис для m дорівнює $z = S^{-1}({}^t(y_1, \dots, y_o, u_1, \dots, u_v))$.

Перевірка підпису. Підпис z перевіряється, якщо $F(z) = m$ виконується.

Завдяки визначенню G рівняння в (1) є лінійними рівняннями $(y_1, \dots, y_o)$. Потім генерується підпис у часі $O(n^3)$ на UOV. Відомо, що UOV з $o=v$ (збалансована схема підпису олії та оцту [3]) розбита атакою Кіпніса-Шаміра [4, 9]. Основна ідея атаки Кіпніса-Шаміра полягає в наступному: атака Кіпніса-Шаміра. Припустимо, що $o=v$ і, для простоти, S - лінійна карта, виражена матрицею $n \times n$. Нехай $f_1(x), \dots, f_o(x)$ - квадратичні форми у $F(x)$ і G_l , F_l ($1 \leq l \leq o$) - матриці коефіцієнтів $g_l(x)$, $f_l(x)$ відповідно, тобто $g_l(x) = {}^t x G_l x +$ (лінійна форма x), $f_l(x) = {}^t x F_l x +$ (лінійна форма x). За визначеннями G , F витікає наступне

$$G_l = \begin{pmatrix} 0_o & * \\ * & *_{vv} \end{pmatrix}, F_l = {}^t S G_l S = {}^t S \begin{pmatrix} 0_o & * \\ * & *_{vv} \end{pmatrix} S.$$

з тих пір

$$\begin{pmatrix} 0_o & * \\ * & *_{vv} \end{pmatrix}^{-1} \begin{pmatrix} 0_o & * \\ * & *_{vv} \end{pmatrix} = \begin{pmatrix} *_{oo} & * \\ 0 & *_{vv} \end{pmatrix}$$

маємо

$$W_1^{-1}W_2 = S^{-1} \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} S$$

для двох лінійних сум W_1 та W_2 $F_1, \dots, F_o$. Відомо, що зломисник може відновити незворотну матрицю $n \times n$ S_1 так, що $SS_1 = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ в поліноміальний час лінійним алгебраїчним підходом на $W_1^{-1}W_2$ (детальніше див. [9]). Після відновлення такої матриці S_1 зломисник може створювати фіктивні підписи з тих пір

$${}^tS_1F_1S_1 = {}^t(SS_1)G_1(SS_1) = \begin{pmatrix} 0 & * \\ * & * \end{pmatrix}$$

Коли $v > o$, оригінальна атака Кіпніса-Шаміра [9] відтоді недоступна

$$\begin{pmatrix} 0 & * \\ * & * \end{pmatrix}^{-1} \begin{pmatrix} 0 & * \\ * & * \end{pmatrix} \neq \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

Ця атака була організована в [4], щоб бути доступною також для $v > o$. Однак її складність – це вже не поліноміальний час, а $O(q^{v-o})$ (полін.). Параметр v , таким чином, приймається достатньо більшим, ніж o для побудови захищеної UOV.

3. CIRCULANT UOV

Нижче розглянемо побудову Circulant UOV (C-UOV, коротше) [7], варіант UOV.

Для $1 \leq l \leq o$, нехай A_l, B_l - $v \times o$ - і $v \times v$ - матриці відповідно, $c_l \in F_q^n$ - вектор рядка, а $d_l \in F_q$ такий, що $g_l(x) = {}^t x \begin{pmatrix} 0 & {}^t A_l \\ A_l & B_l \end{pmatrix} x + c_l x + d_l$. У оригіналі UOV A_l, B_l, c_l, d_l вибираються випадковим чином. З іншого боку в Circulant UOV, A_l і c_l наведено наступним чином.

$$\begin{cases} A_1 = (a_1, a_2, a_3, \dots, a_o) \\ A_2 = (a_o, a_1, a_2, \dots, a_{o-1}) \\ A_3 = (a_{o-1}, a_o, a_1, \dots, a_{o-2}) \\ \vdots \\ A_o = (a_2, a_3, a_4, \dots, a_o, a_1) \\ c_1 = (c_1, c_2, c_3, \dots, c_o, c_{o+1}^{(1)}, c_n^{(1)}) \\ c_2 = (c_o, c_1, c_2, \dots, c_{o-1}, c_{o+1}^{(2)}, c_n^{(2)}) \\ c_3 = (c_{o-1}, c_o, c_1, \dots, c_{o-2}, c_{o+1}^{(3)}, c_n^{(3)}) \\ \vdots \\ c_o = (c_2, c_3, c_4, \dots, c_o, c_1, c_{o+1}^{(o)}, c_n^{(o)}) \end{cases} \quad (2)$$

де $a_1, \dots, a_o \in F_q^v$ – це вектори стовпців, а $c_1, \dots, c_o, c_{o+1}^{(1)}, \dots, c_n^{(o)} \in F_q$ – постійні, B_l, d_l випадкові. Для таких A_l, c_l лінійні рівняння (1), розв'язані в процесі генерації підпису UOV, задаються

$$\begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_o \\ a_o & a_1 & a_2 & \dots & a_{o-1} \\ a_{o-1} & a_o & a_1 & \dots & a_{o-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_2 & a_3 & a_4 & \dots & a_1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_o \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \\ \vdots \\ \beta_o \end{pmatrix}, \quad (3)$$

для констант $\alpha_1, \dots, \alpha_o, \beta_1, \dots, \beta_o \in F_q$ залежно від $u_1, \dots, u_v$. Матриця в лівій частині рівняння (3) є матрицею „circulant”, і, як відомо, вона інвертується в часі $O(n^2)$ (див., Наприклад, [10]), що швидше, ніж $O(n^3)$ для випадкової матриці. Таким чином, генерація сигнатур Circulant UOV швидше, ніж оригінальна UOV

4. АТАКА КІПНІСА-ШАМІРА НА C-UOV

Вхідні дані: Коефіцієнти матриць $F_1, \dots, F_o$ квадратичних форм $f_1(x), \dots, f_o(x)$.

Вихід: обернена лінійна карта $S_1: F_q^n \rightarrow F_q^n$ така, що $SS_1 = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$

Крок 1. Візьміть дві лінійні суми W_1, W_2 $F_1, \dots, F_o$ таким чином, що W_1 є зворотним. Обчисліть $W := W_1^{-1}W_2$.

Крок 2. Обчисліть характерний многочлен $w(t) := \det(t \cdot I_n - W)$ W і коефіцієнт $w(t) = w_1(t)^2 w_2(t)$ двома поліномами $w_1(t), w_2(t)$ ступеня o і $v-o$ відповідно. Якщо $w_2(t)$ не є квадратним, поверніться до кроку 1 та змініть W_1, W_2 .

Крок 3. Обчисліть $w_1(W)$ і візьміть обернену матрицю $n \times n$ S^{-1} такий, що $w_1(W)$

$$S^{-1} = \begin{pmatrix} 0 & * \\ * & *_{\nu} \end{pmatrix}$$

Крок 4. Виведіть $S_1 = S^{-1}$.

$$W = S^{-1} \begin{pmatrix} W_1 & * \\ 0 & *_{\nu} \end{pmatrix} S$$

для деякої $o \times o$ матриці W_1 . Тоді існують многочлени $w_1(t)$, $w_2(t)$, як наведено на кроці 2. Оскільки, якщо $w_2(t)$ квадратне, характерний многочлен $\det(t \cdot I_o - W_1)$ W_1 визначається однозначно $w_1(t)$, це справедливо

$$w_1(W) = S^{-1} \begin{pmatrix} W_1 & * \\ 0 & *_{\nu} \end{pmatrix} S$$

Можемо легко перевірити, що S^{-1} на кроці 3 задовольняє $SS^{-1} = \begin{pmatrix} 0 & * \\ 0 & *_{\nu} \end{pmatrix}$

Атака, описана вище, відбувається в поліномічний час, оскільки включає лише основні лінійні операції. У таблиці 1 описані результати експериментів атаки Кіпніса-Шаміра проти Circulant UOV на Magma [11] ver.22-3 для Windows 8.1, Core (TM) i7-4800MQ, 2.70 ГГц для параметрів вибрано в [7] як 80-, 100- та 120-бітні параметри безпеки. Зауважимо, що в цих параметрах числа m квадратичних форм у F не збігаються з o , оскільки на Circulant UOV застосовано „мінус” (див. П. 5 [7]). Неважко помітити, що „мінус” не заважає атаці Кіпніса-Шаміра. Завдяки результатам цієї таблиці ми можемо зробити висновок, що Circulant UOV взагалі не захищений від нападу Кіпніса-Шаміра.

Таблиця 1

Атака Кіпніса-Шаміра на C-UOV.

q	n	m	o	v	Час, сек	Параметри безпеки, біт
31	99	33	34	65	0,59	80
31	123	41	43	80	1,64	100
31	156	52	53	103	6.54	128

Зауважимо, що необхідні подальші обговорення у випадку, якщо поле F_q є навіть характерним. Коли q парне, матриці коефіцієнтів $F_1, \dots, F_o$ не можуть бути симетричними, і тоді зломисник використовує $F_1 + {}^tF_1$ замість самого F_1 . Такі матриці є симетричними, а також косими симетричними. Для двох $n \times n$ кососиметричних матриць R_1, R_2 відомо, що матриці R_1, R_2 не є зворотними, якщо n непарне, а мінімальний многочлен $R^{-1}_1 R_2$ має ступінь $n/2$ якщо n парне (див., наприклад, [12–14]). Це означає, що напад, запропонований у цьому розділі, не доступний безпосередньо для навіть характерних випадків, і ми мусимо домогтися того, щоб він був доступним і для навіть характерних випадків у майбутньому.

Також зауважуємо, що якщо A_1 не є повноцінним, крок 1 атаки завжди провалюється, оскільки W^{-1}_1 не існує. Однак у такому випадку зломисник може відновити часткову інформацію S . Коли ранг A_1 , наприклад, $o-1$, існує неперевернена матриця $o \times o$ D та $v \times (o-1)$ матриця A' такі, що $A_1 = (0, A')$ D і тоді $F_1 = S \begin{pmatrix} D & \\ & I_{\nu} \end{pmatrix} \begin{pmatrix} 0 & \\ & *_{n-1} \end{pmatrix} \begin{pmatrix} D & \\ & I_{\nu} \end{pmatrix} S$ утримує. Можемо відновити $n \times n$ матрицю S_0 за допомогою $\begin{pmatrix} D & \\ & I_{\nu} \end{pmatrix} S S_0 \begin{pmatrix} *_1 & * \\ 0 & *_{n-1} \end{pmatrix}$ елементарними лінійними операціями на F_1 . Неважко помітити, що щойно такий S_0 заданий, можна зменшити задачу відновлення ключа, еквівалентного (o, ν) -UOV, клавійші $(o-1, \nu)$ -UOV, взявши нижчу- справа $(n-1) \times (n-1)$ малі матриці ${}^tS_0 F_1 S_0, \dots, {}^tS_0 F_o S_0$. Це означає, що зломисник може відновити еквівалентний ключ, застосувавши атаку на таких матрицях меншого розміру.

5. RAINBOW TA CIRCULANT RAINBOW

Rainbow [5] - багат шарова версія UOV. Розглянемо двошарову версію.

Нехай $o_1, o_2, v, n, m \geq 1$ - цілі числа з $n = o_1 + o_2 + v$, $m = o_1 + o_2$. Визначте квадратичну карту $G: F_q^n \rightarrow F_q^m$

Схема підпису Rainbow будується наступним чином.

Секретний ключ. Дві обернені афінні карти $S: F_q^n \rightarrow F_q^n$, $T: F_q^m \rightarrow F_q^m$ і квадратична карта G , визначена вище.

Публічний ключ. Квадратична карта $F: F_q^n \rightarrow F_q^o$

Генерація підписів. Для повідомлення $m \in F_q^m$, яке слід підписати, нехай $w = {}^t(w_1, \dots, w_m) = T^{-1}(m)$. Вибираємо $u_1, \dots, u_v \in F_q$ випадковим чином і знаходимо $(y_{o_1+1}, \dots, y_m) \in F_q^{o_2}$

$$\begin{aligned} g_{o_1+1}(y_1, \dots, y_m, u_1, \dots, u_v) &= w_{o_1+1} \\ \dots, g_m(y_1, \dots, y_m, u_1, \dots, u_v) &= w_{o_1+1} \end{aligned} \quad (4)$$

Після цього знаходимо $(y_1, \dots, y_{o_1}) \in F_q^{o_1}$

$$\begin{aligned} g_1(y_1, \dots, y_m, u_1, \dots, u_v) &= w_1 \\ \dots, g_{o_1}(y_1, \dots, y_m, u_1, \dots, u_v) &= w_{o_1} \end{aligned} \quad (5)$$

Підпис для m дорівнює $z = S^{-1}({}^t(y_1, \dots, y_m, u_1, \dots, u_v))$.

Перевірка підпису. Підпис z перевіряється, якщо $F(z) = m$ виконується.

Зауважимо, що (4) – система o_2 лінійних рівнянь o_2 змінних $y_{o_1+1}, \dots, y_m$ і (5) – система o_1 лінійних рівнянь o_1 змінних $y_1, \dots, y_{o_1}$.

Матриці коефіцієнтів $G_1, \dots, G_m$ $g_1(x), \dots, g_m(x)$ записуються через

$$G_j = \begin{cases} \begin{pmatrix} 0_{o_1} & {}^tA_j \\ A_j & B_j \end{pmatrix}, & (1 \leq j \leq o_1) \\ \begin{pmatrix} 0_{o_1} & 0 & 0 \\ 0 & 0_{o_2} & {}^tC_j \\ 0 & C_j & D_j \end{pmatrix}, & (o_1 + 1 \leq j \leq m) \end{cases}$$

де A_j, B_j, C_j, D_j – $(o_2+v) \times o_1$ -, $(o_2+v) \times (o_2+v)$ -, $v \times o_2$ - і $v \times v$ - матриці відповідно. Аналогічно UOV, коефіцієнти матриць $F_1, \dots, F_m$ $f_1(x), \dots, f_m(x)$ задаються

$$F_j = {}^tS \begin{pmatrix} 0_o & * \\ * & *_{o_2+v} \end{pmatrix} S$$

і тоді складність атаки Кіпніса-Шаміра на вихідну Rainbow становить $O(q^{o_2+v-o_1} \cdot (\text{полін.}))$. У Circulant Rainbow [8] вище вибираються матриці A_j, C_j аналогічно (2), а потім системи лінійних рівнянь (4), (5) у поколінні сигнатур записуються також матрицями циркуляції, подібними до (3). Таким чином, генерація підписів Circulant Rainbow швидше, ніж у оригінальної Rainbow. Однак, як і Circulant UOV, зломисник може відновити обернену лінійну карту $S_1: F_q^n \rightarrow F_q^n$ так, що $SS_1 = \begin{pmatrix} 0_o & * \\ * & *_{o_2+v} \end{pmatrix}$ атакою Кіпніса-Шаміра, наведеним у п.4. Неважко помітити, що після відновлення такого S_1 зломисник може відновити подальшу інформацію про S і T , що є достатньою для генерування фіктивних підписів для довільних повідомлень (див., Наприклад, [15]). Таким чином робимо висновок, що Circulant Rainbow також не є безпечним.

6. ВИСНОВОК Circulant UOV [7] та Circulant Rainbow [8] – це нові варіанти UOV [3,4] та Rainbow [5]. Ці варіанти використовують „циркуляційні” структури в квадратичних формах для прискорення поколінь підписів UOV та Rainbow. Однак, як описано в п.4, такі циркуляційні структури критично послаблюють безпеку, особливо проти нападу Кіпніса-Шаміра [4, 9]. Ця ситуація схожа на ELSA, інший швидкий варіант Rainbow, запропонований на Asiacrypt 2017 [16] та розбитий на IWSEC 2018 [17]. Таким чином, вважаємо, що треба досить уважно вивчати безпеку, коли намагаємося підвищити ефективність цих схем.

ЛІТЕРАТУРА

1. A.S.Fraenkel and Y.Yesha, Complexity of problems in games, graphs and algebraic equations, Discrete Appl. Math., 1 (1979), 15 – 30.
2. M.R. Garey and D.S. Johnson, Computers and Intractability: A Guide to the Theory of NP completeness, W. H. Freeman, New York, 1979.
3. J. Patarin, The Oil and Vinegar Signature Scheme, the Dagstuhl Workshop on Cryptography, 1997.

4. A.Kipnis, J.Patarin and L.Goubin, Unbalanced oil and vinegar signature schemes, in: Proc.of EUROCRYPT '99, J.Stern ed., LNCS, Vol. 1592, pp. 206 – 222, Springer, Berlin, Heidelberg, 1999, extended in <http://www.goubin.fr/papers/OILLONG.PDF>, 2003.
5. J.Ding and D.Schmidt, Rainbow, a new multivariate polynomial signature scheme, in: Proc. Of ACNS 2005, J. Ioannidis et al. eds., LNCS, Vol. 3531, pp. 164 – 175, Springer, Berlin, Heidelberg, 2005.
6. NIST, Post-quantum cryptography standardization, <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization>.
7. Z.Peng and S.Tang, Circulant UOV: a new UOV variant with shorter private key and faster signature generation, KSII T. Internet Info., 12 (2018), 1376 – 1395.
8. Z. Peng and S. Tang, Circulant Rainbow: A new Rainbow variant with shorter private key and faster signature generation, IEEE Access, 5 (2007), 11877 – 11886.
9. A. Kipnis and A. Shamir, Cryptanalysis of the oil and vinegar signature scheme, in: Proc.of CRYPTO '98, H.Krawczyk ed., LNCS, Vol. 1462, pp. 257 – 267, Springer, Berlin, Heidelberg, 1998.
10. I. Kra and S. R. Simanca, On circulant matrices, Notices of the AMS, 59 (2012), 368–377.
11. W. Bosma, J. Cannon and C. Playoust, The Magma algebra system.I.The user language, J.Symbolic Comput., 24 (1997), 235 – 265.
12. A. Cayley, Sur les determinants gauches (On skew determinants), J. Reine Angew. Math, 38 (1847), 93 – 96.
13. D.Z. Doković, On the product of two alternating matrices, Amer. Math. Monthly, 98 (1991), 935 – 936.
14. O. Taussky and H. Zassenhaus, On the similarity transformation between a matrix and its transpose, Pacific J. Math., 9, (1959), 893 – 896.
15. B.Y. Yang and J.M. Chen, Building secure tame-like multivariate public-key cryptosystems: the new TTS, in: Proc. Of ACISP '05, C. Boyd et al. eds, LNCS, Vol. 3574, pp. 518–531, Springer, Berlin, Heidelberg, 2005.
16. K.-A. Shim, C.-M. Park and N. Koo, An existential unforgeable signature scheme based on multivariate quadratic equations, in: Proc. of ASIACRYPT '17, T. Takagi et al. eds, LNCS, Vol. 10624, pp. 37 – 64, Springer, Cham, 2017.
17. Y. Hashimoto, Y. Ikematsu and T. Takagi, Chosen message attack on multivariate signature ELSA at Asiacypt 2017, in: Proc. of IWSEC '18, A. Inomata et al. eds, LNCS, Vol. 11049, pp. 3 – 18, Springer, Cham, 2018.

АРХІТЕКТУРНІ РІШЕННЯ ДЛЯ РОЗРОБКИ СИСТЕМИ ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ ЗБРОЙНИХ СИЛ УКРАЇНИ

Рівень готовності Збройних Сил України до виконання завдань за призначенням безпосередньо залежить від наявності новітнього озброєння і військової техніки, але жодне озброєння і техніка не можуть забезпечити ефективного виконання бойових задач без своєчасного, достовірного та безпечного управління військами та озброєнням.

В рамках реалізації положень Стратегічного оборонного бюлетеня України керівництвом ЗС України ведеться робота щодо створення ефективної системи оперативного управління, зв'язку, розвідки та спостереження (C4ISR). Головною вимогою впровадження систем типу C4ISR є відповідність стандартам НАТО.

Разом з тим, при впровадженні такого роду систем у існуючу структуру системи управління військами (силами) та озброєнням необхідно враховувати особливості функціонування систем військового призначення, процеси, які відбуваються в них, завдання, що покладаються до виконання тими чи іншими підсистемами. Це призводить до необхідності вирішення актуального завдання, пов'язаного з вибором доцільного архітектурного рішення майбутньої системи зв'язку та інформатизації ЗС України, яке б враховувало основні сучасні принципи, концепції, правила та стандарти побудови інформаційних систем, у тому числі з урахуванням стандартів НАТО.

У ході дослідження, завдання щодо вибору доцільного архітектурного рішення майбутньої системи зв'язку та інформатизації ЗС України вирішувалося на двох рівнях: архітектурні рішення високого та технічного рівнів. Розглянемо детальніше особливості запропонованих рішень. Архітектура високого рівня (*Enterprise Architecture* – ЕА) – це спосіб формалізації проблем зацікавлених сторін та їх представлення в контексті організації. Зокрема, ЕА повинна охоплювати як організаційні, так і технічні поняття майбутньої архітектури зв'язку та інформатизації, щоб підкреслити залежності між ними і сформулювати цілісний підхід для управління процесами, пов'язаними із системою інтересів посадових осіб (підрозділів) пунктів та органів у системі управління ЗС України.

На практиці, архітектура високого рівня будується на основі аналізу структури тієї чи іншої організації та процесів які відбуваються в ній. В результаті такого аналізу формується модель архітектури яка забезпечує ефективність, продуктивність, гнучкість та стійкість системи, що має за мету оптимізувати як зазначені процеси (як вручну, так і в автоматизованому режимі) так і систему в цілому.

На рис. 1 зображеного варіант архітектури високого рівня на прикладі взаємодії клієнта з додатком, який надає певні послуги. З рисунку видно, що клієнт на пряму не взаємодіє з сервісами, а тільки з використанням спеціального інтерфейсу взаємодії (API, Web-інтерфейс). При створенні складних, розподілених інформаційних систем, проектуванні їх архітектури, розробці інфраструктурних рішень, виборі компонентів і зв'язків між ними, слід враховувати, крім загальних (відкритість, масштабованість, переносимість, мобільність, захищеність, тощо), низку специфічних концептуальних вимог: висока доступність, кросплатформенність, масштабованість, відмовостійкість, безпека, гнучкість.

На сьогоднішні існує велика кількість архітектурних рішень для побудови різного роду інформаційних та телекомунікаційних систем. Найбільш популярними на даний час є:

- *монолітна архітектура*: системи з використанням монолітної архітектури будуються як єдине ціле. Будь які зміни, навіть найменші, потребують перебудови та розгортання всього додатку. З часом стає складніше зберігати модульну структуру системи, відтак як зміни логіки одного модуля впливають на код інших модулів. Монолітні програми також важко масштабувати, коли різні модулі мають конфліктні вимоги до ресурсів.

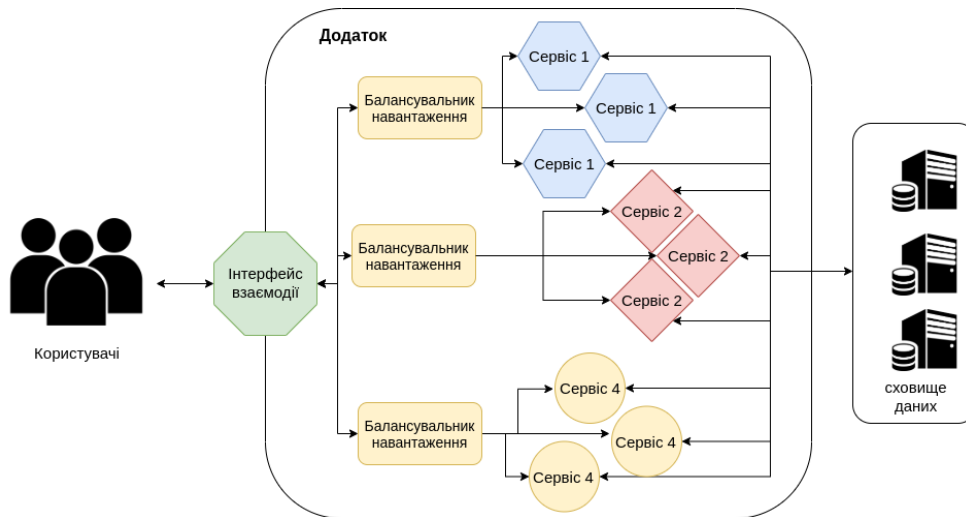


Рис. 1 Приклад архітектури високого рівня

– *сервісно-орієнтована (Service-oriented architecture, SOA)*: це підхід до розробки інформаційних систем, при якому сервіси надаються іншим компонентам додатку через стандартні мережеві протоколи. Тобто, розміщені в мережі (хмарі) сервіси взаємодіють один з одним та надають користувачам певні послуги шляхом використання тих чи інших застосунків (обміну повідомленнями) для зв'язування сервісів, а не написання нового програмного коду. У разі зміни структури чи мети функціонування організації чи її елементів, достатньо буде перелаштувати процес обміну повідомленнями між існуючими сервісами, а не розробляти нове програмне забезпечення для реалізації існуючих сервісів.

– *мікросервісна архітектура*: це підхід до побудови архітектури, за якого інформаційна система складається з множини взаємопов'язаних сервісів, кожен з яких функціонує у своєму власному процесі та комунікує з рештою процесів, використовуючи механізм HTTP. Подібні сервіси будують у залежності від потреб користувачів і розгортаються незалежно один від одного, з використанням повністю автоматизованого середовища. Зростаюча складність систем, навантаження на окремі її частини, а також необхідність відповідати сучасним вимогам до побудови сервісів, створюють потребу в нових, гнучких підходах до проектування програмного забезпечення та інфраструктури для його розгортання. З урахуванням того, що сучасні сервіси будуються з використанням різних мов програмування і технологій зберігання даних, мікросервісна архітектура підходить для процесів безперервного постачання одного чи кількох застосунків, необхідних кінцевому користувачеві, на відміну від сервісно-орієнтованої архітектури.

У результаті аналізу вищезазначених архітектурних рішень, у ході дослідження було запропоновано багаторівневу модель системи зв'язку та інформатизації високого рівня з використанням мікросервісного архітектурного підходу (рис. 2).

На рівні збору інформації реалізовано сервіси збору (за допомогою використання сенсорів, трекерів, безпілотних літальних апаратів, супутників, тощо) та відображення інформації про усі сфери життєдіяльності як Збройних Сил (в умовах повсякденної діяльності та умовах особливого періоду), так і суспільства в цілому. При цьому, для отримання повної ситуаційної обізнаності посадовими особами органів військового управління передбачається наявність інтерфейсів для взаємодії інформаційних систем ЗС України з системами інших структур силового блоку держави.

Рівень обробки інформації передбачає наявність технологій та методів зберігання та аналізу як структурованих, так і неструктурованих даних, у тому числі машинного навчання та обробки великих масивів даних (Big Data), за допомогою яких здійснюється отримання якісно нових знань. Кінцевою метою цієї обробки є подання інформації у формі, яка забезпечить зручність сприйняття відповідними посадовими особами в умовах неперервного

росту й поширення інформації між численними вузлами, які входять до складу інформаційних систем.

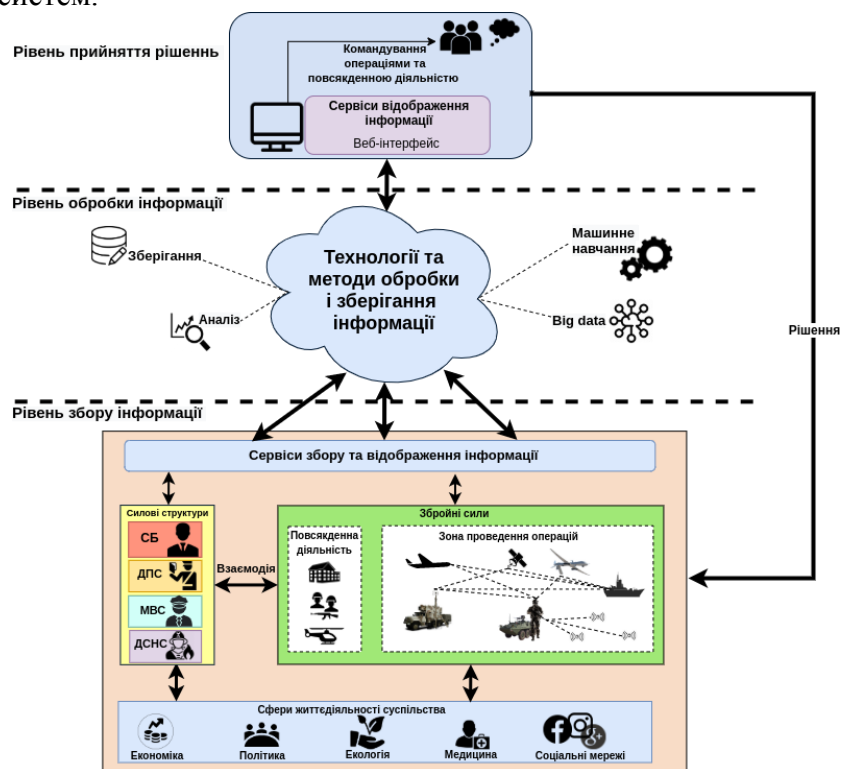


Рис. 2 Архітектура системи зв'язку та інформатизації високого рівня

На рівні прийняття рішень повинен забезпечуватися доступ посадових осіб до сервісів та інформаційних ресурсів, які розміщені на нижніх рівнях архітектури. Реалізація доступу відбувається з використанням веб-інтерфейсу, засобами якого буде реалізовано ідентифікацію користувача, а також перевірка прав його доступу до ресурсів системи.

Зазначена архітектура відображає в собі всі етапи циклу управління, починаючи від збору інформації про стан об'єктів управління (та з інших сфер життєдіяльності), її передачі і в подальшому зберігання, аналіз, систематизацію та, у разі необхідності, формування варіантів розвитку подій (альтернатив) на базі яких посадові особи будуть приймати рішення та віддавати накази (рис. 3).

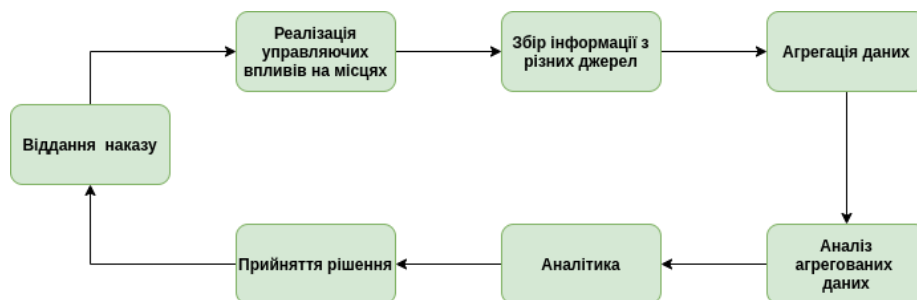


Рис. 3 Цикл управління, який реалізується в архітектурі високого рівня

При розробці такого роду систем не менш важливим питанням є вибір технічної складової (технічної архітектури), яка зможе забезпечити надійне, відмовостійке, безпечне і продуктивне середовище функціонування усіх підсистем.

Технічна архітектура (*Technical Architecture* – ТА) є першим рівнем загальної архітектури інформаційної системи та складає її основу (базис). Вона описує всі апаратні засоби, що використовуються при виконанні заявленого набору функцій, а також включає засоби забезпечення мережевої взаємодії та надійності. Іншими словами, технічна

архітектура – це сукупність програмно-апаратних засобів, методів та стандартів, які забезпечують ефективне функціонування системи та описують повне представлення інфраструктури в цілому.

Важливим аспектом на етапі проектування інформаційних систем та системи зв'язку в цілому є вибір технологічного рішення за допомогою якого майбутня або існуюча система буде виконувати ті вимоги, які висуваються до неї та завдання, які на неї покладаються.

На сьогодні існує низка технологій, на основі яких здійснюється побудова різного роду систем, в тому числі зв'язку та інформатизації. Зокрема великий технологічний стрибок здійснили хмарні технології, які, в свою чергу, базуються на використанні різних архітектур. Розглянемо їх детальніше.

Хмарні архітектури – у найзагальнішому вигляді хмари для великих і середніх за розміром організацій (як комерційних компаній, так і державних структур) можна розділити на три основні типи:

- публічні (*Public Cloud*);
- приватні (*Private Cloud*);
- гібридні (*Hybrid Cloud*).

Кожен з них має характерні переваги та недоліки. Публічна хмара надає обчислювальні ресурси власного дата-центру великій кількості незалежних користувачів для розміщення власних додатків. Приватна хмара – повністю знаходиться в управлінні однієї організації. Гібридний підхід об'єднує в собі дві перші концепції, отримуючи від кожної з них основні переваги і деякі недоліки. Розглянемо їх детальніше.

Публічна хмара. На сьогодні це найпоширеніша концепція надання хмарних послуг. В даному випадку вся IT-інфраструктура розміщується у сервіс-провайдері (компанії, яка надає сервіс). Такий оператор самостійно закуповує або орендує сервери, системи зберігання даних, мережеве обладнання та інші апаратні компоненти, а також підтримує, модернізує і оновлює всі системи в міру необхідності. При цьому сервіс-провайдер надає хмарні послуги великій кількості незалежних замовників, які спільно використовують одну і ту ж IT-інфраструктуру, що знаходиться під його управлінням і контролем. Організація-клієнт, в свою чергу, отримує доступ до необхідного обсягу IT-ресурсів за певну абонентську плату.

Переваги:

- просте та ефективне використання;
- технологічна та фінансова гнучкість;
- економія витрат на інфраструктуру;
- використання IT-послуг тільки в необхідному обсязі (відсутність переоплат);
- легке масштабування;
- швидка реакція на пікові навантаження;
- надійність та відмовостійкість;
- новітнє обладнання і ПЗ.

Недоліки:

- контроль IT-інфраструктури сторонньою компанією (сервіс-провайдер);
- залежність від швидкості і стабільності доступу до мережі Інтернет;
- потреба у постійному оновленні підходів щодо захисту даних за межами внутрішнього периметру кібербезпеки.

Приватна хмара. У приватній хмарі, на відміну від публічної, вся обчислювальна інфраструктура знаходиться під повним контролем самої організації. По суті, мова йде про гнучку, глибоко віртуалізовану платформу, ресурси якої знаходяться в розпорядженні однієї організації. Фізично IT-інфраструктура може розміщуватися у власному дата-центрі. Нерідко трапляється ситуація, коли приватна хмара являє собою мережу з декількох корпоративних дата-центрів.

Переваги:

- висока швидкість роботи;
- високий рівень безпеки;

- ексклюзивне використання ресурсів однієї компанії;
- повний контроль обладнання та ПЗ.

Недоліки:

- значні фінансові витрати на етапі побудови;
- потреба у висококваліфікованих фахівцях;
- витрати на модернізацію та оплату ПЗ;
- необхідність точного планування навантаження на майбутні роки.

Гібридна хмара. Передбачає поєднання власного дата-центру з дата-центром сервіс-провайдера. У якості прикладу можна навести системи, в яких розміщення додатків проводиться на ресурсах сервіс-провайдера, а збереження даних відбувається у власному дата-центрі.

На практиці всі вищезазначені типи хмарних архітектур можуть бути реалізовані з використанням різного роду моделей, найрозповсюдженішими серед яких на сьогодні є IaaS, PaaS та SaaS (рис. 4). Розглянемо їх детальніше.

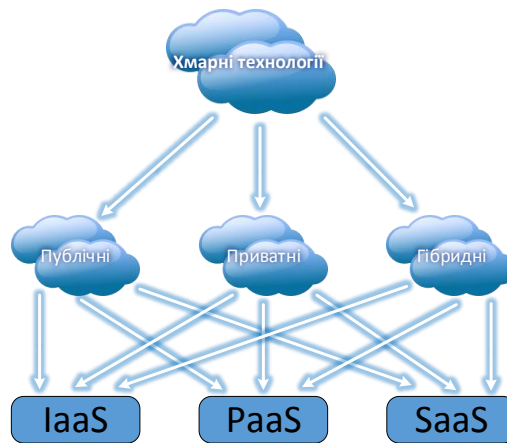


Рис. 4 Моделі хмарних архітектур

IaaS (Infrastructure-as-a-Service) – використання даної моделі передбачає надання користувачеві інформаційно-технологічних ресурсів (віртуальних серверів) з певною обчислювальною потужністю та обсягами пам'яті. За налаштування та підтримання в працездатному стані апаратного забезпечення відповідає провайдер. Він встановлює на нього ПЗ для створення віртуальних машин, але не займається установкою і підтримкою ПЗ користувача. Провайдер контролює тільки фізичну та віртуальну інфраструктуру. Приклади IaaS: IBM Softlayer, Hetzner Cloud, Microsoft Azure, Amazon EC2, GigaCloud.

Користувачі IaaS – це системні адміністратори організацій.

PaaS (Platform-as-a-Service) – провайдер надає доступ користувачам до операційних систем, засобів розробки і тестування, систем управління базами даних. На відміну від моделі IaaS, провайдер контролює не тільки віртуальні сервери, системи зберігання даних і обчислювальні потужності, але також пропонує користувачеві на вибір певні платформи і засоби управління ними. Приклади PaaS: Google App Engine, IBM Bluemix, Microsoft Azure, VMWare Cloud Foundry.

Основні користувачі PaaS-сервісів – це розробники ПЗ.

SaaS (Software-as-a-Service) – одна з найпоширеніших хмарних моделей, за якої програми та сервіси розробляє і обслуговує провайдер, розміщує їх в хмарі і пропонує до використання кінцевому користувачеві через браузер або веб-додаток на його ПК. Користувач лише вносить абонплату (або користується сервісом безкоштовно), оновленням і технічною підтримкою програм займається провайдер. SaaS-сервіси можуть надавати місце для зберігання файлів (Dropbox), офісний пакет документів для роботи (Google Doc, Microsoft Office 365), допомагати організовувати фотографії (Flickr) або спілкуватися з іншими людьми (Facebook).

Основними клієнтами SaaS-сервісів є кінцеві користувачі.

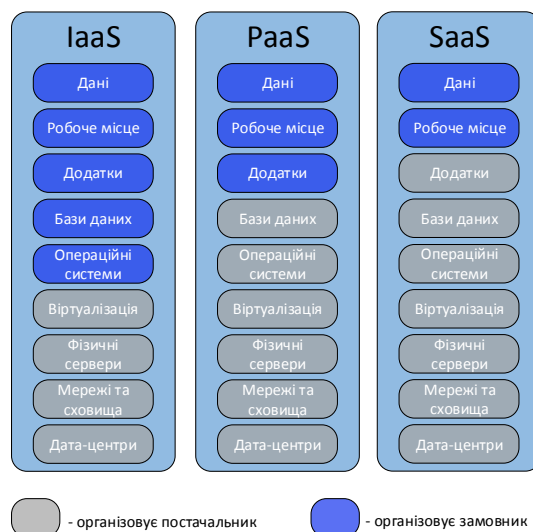


Рис. 5 Сервіси, які забезпечуються різними хмарними архітектурами

В свою чергу вищезазначені хмарні архітектури не можуть функціонувати без належного рівня підтримки та адміністрування. У відповідності до цього нижче представлено приклади моделей хмарних архітектур та відповідні фахівці, які мають здійснювати управління ними.

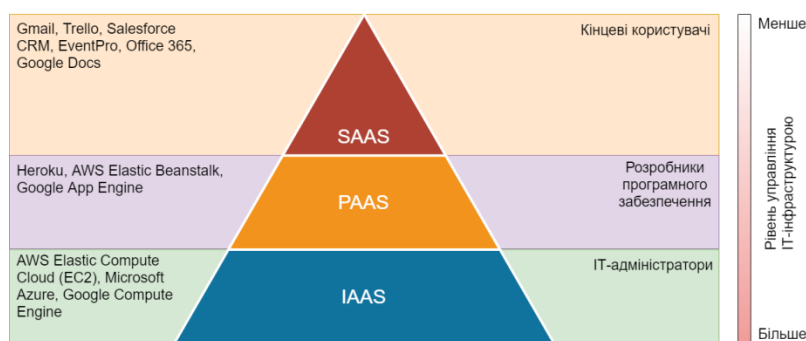


Рис. 6. Приклади моделей хмарних архітектур у залежності від рівня управління ними

Таким чином, модернізація мереж зв'язку та інформатизації Збройних Сил України потребує використання новітніх архітектурних і технічних рішень з метою забезпечення сумісності національних систем із системами, побудованими за стандартами НАТО.

Запропонована в ході дослідження модель архітектури системи зв'язку та інформатизації високого рівня може стати основою для створення систем типу C4ISR в ЗС України. Практична реалізація рівнів моделі дозволить скоротити час на прийняття рішень та підвищити якість управлінських рішень посадовими особами в системі управління військами та озброєнням, шляхом надання доступу зазначених посадових осіб до інформаційних ресурсів відповідно до їх повноважень, що відповідає сучасним тенденціям зі створення інформаційних систем за стандартами НАТО.

Разом з тим, при розробці вищезазначеної системи зв'язку та інформатизації стає актуальним питання вибору тієї чи іншої моделі технічної архітектури, що залежить від конкретних завдань, які ставляться до виконання перед тим чи іншим підрозділом чи органом управління, їх організаційної структури та ресурсів (матеріальних та людських). З огляду на особливості функціонування інформаційних систем спеціального призначення, пропонується використання гібридної хмарної архітектури.

У ході подальших досліджень буде розроблено методи та моделі обміну інформацією у розподілених інформаційних системах спеціального призначення зі змінною топологією.

ВИКОРИСТАННЯ НОВІТНІХ ТЕХНОЛОГІЙ У РОЗРОБЦІ ВИСОКОТЕХНОЛОГІЧНОЇ ЗБРОЇ

Досягнення інформаційно-технічної революції були використані для створення високоточної зброї, інформаційних систем та засобів військового призначення, проривних досліджень у військовій радіоелектроніці. Саме її досягнення є тією основою, на якій будується вся система озброєння сучасної армії. Це в свою чергу зумовило і зміну підходів до ведення війни і основам будівництва збройних сил.

Відмінна особливість розвитку засобів збройної боротьби в сучасних умовах полягає в появі якісно нових видів зброї, такої як високоточна зброя, зброя на нових фізичних принципах, інформаційна зброя, зброя на основі роботизованих систем.

При цьому інформатизація засобів збройної боротьби дозволила створити не тільки глобальні системи розвідки, зв'язку і навігації, а й взаємопов'язати різні засоби озброєння, розвідки і пункти управління в єдину інформаційно-мережеве середовище, що дозволило різко збільшити бойові можливості нових видів зброї. В умовах такого об'єднання озброєнь в єдиний інформаційний простір була висунута концепція мережецентричної війни як стратегічного погляду на ведення війни в нових військово-технічних умовах. Ця концепція не обмежується розробкою нових способів застосування озброєнь, а передбачає докорінної зміни організаційних форм збройних сил і способів ведення військових дій всіх масштабів.

«Мережецентрична» війна.

За своєю суттю «мережецентрична» війна - це орієнтована на досягнення інформаційної переваги концепція організації управління діями угруповань військ (сил), що передбачає збільшення їх бойової могутності за рахунок створення єдиної інформаційно-комутаційної мережі, що зв'язує датчики (джерела даних), осіб, які приймають рішення і виконавців, що забезпечує доведення до учасників дій необхідної інформації про обстановку, прискорення процесу управління силами і засобами, і підвищення, внаслідок цього, темпів операцій і ефективності ураження противника.

На думку розробників концепції, «мережецентричний» спосіб ведення бойових дій дозволяє також перейти від війни на виснаження до більш швидкоплинної і більш ефективної форми ведення збройної боротьби, для якої характерні швидкість управління і принцип самосинхронізації, тобто здатність військової структури самоорганізовуватися знизу, не чекаючи вказівок зверху.

У концептуально-теоретичному плані модель «мережецентричної» війни представляють як систему, що складається з трьох підсистем (рисунок 1), що мають структуру решітки:

- інформаційної підсистеми,
- сенсорної (розвідувальної) підсистеми,
- бойової підсистеми (підсистеми окремих тактичних підрозділів і бойового управління).

Основою системи вважається перша підсистема, на яку накладаються друга і третя підсистеми. Елементами другої підсистеми є сили і засоби розвідки, а третьої - засоби ураження, бойова техніка і особовий склад окремих тактичних підрозділів, об'єднані органами управління та командування.

„Мережецентрична” війна як правило охоплює всі рівні управління, а принципи її ведення не залежать від географічного регіону, бойових завдань, складу і структури збройних сил. Самі ж збройні сили в цьому випадку є розгалуженою мережею добре поінформованих, але географічно розподілених сил.

У найзагальнішому вигляді „мережецентрична” війна передбачає наступні чотири основні фази ведення бойових дій:

1. Досягнення інформаційної переваги за допомогою випереджаючого знищення (виводу з ладу, придушення) системи розвідувально-інформаційного забезпечення супротивника (сенсорів, мережеских вузлів, центрів обробки інформації та управління).
2. Завоювання переваги (панування) в повітрі за рахунок придушення (знищення) системи ППО супротивника на полі бою.
3. Послідовне знищення, залишення без управління та інформації засобів ураження противника, в першу чергу ракетних комплексів, авіації, реактивної і ствольної артилерії, бронетехніки.
4. Остаточне придушення або знищення осередків опору противника.

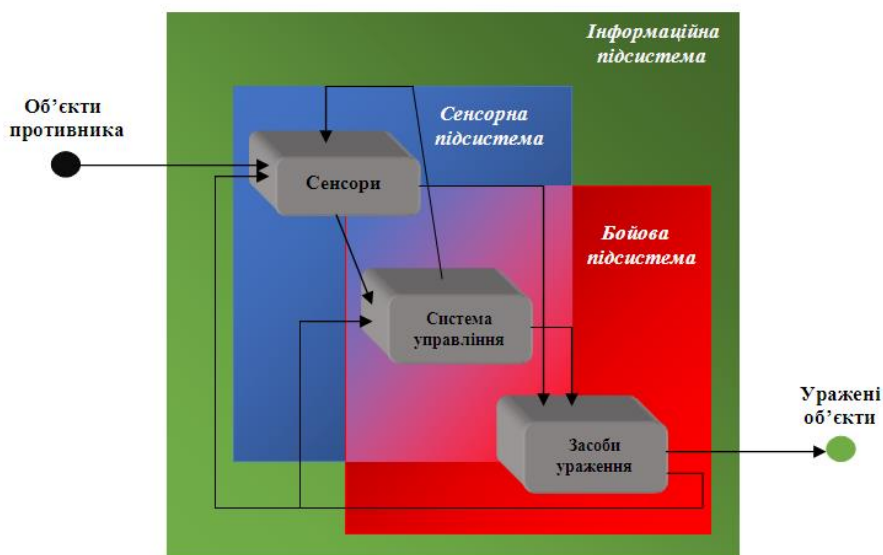


Рис.1. Узагальнена модель концепції „мережецентричної” війни

Таким чином, концепція „мережецентричної” війни передбачає комплексне ведення бойових дій усіма видами і родами збройних сил на основі переваг, які дає використання „єдиного інформаційно-комунікаційного простору” в динаміці бойових дій.

Мозаїчна війна.

Концепція мозаїчної війни на прикладі використання в авіації - масоване застосування пілотованої і безпілотної авіації в тісній зв'язці з наземними і морськими силами, супутниковим угрупованням, комплексами високоточної зброї. Військовий льотчик в цій концепції командує безпілотними літальними апаратами (БПЛА), які виконують основну частину бойових завдань. У момент застосування декількох БПЛА в бойовому порядку з пілотованим винищувачем: один БПЛА ставить заваду ворожим радарам, другий несе озброєння, третій шукає цілі та виконує функцію ретранслятора, четвертий виступає в ролі мішені для засобів ППО. Кількість БПЛА, їх конфігурацію, обладнання та озброєння може змінюватись в залежності від бойового завдання - як елементи мозаїки.

Концепція „мозаїчної війни” вимагає велику кількість недорогих вузькоспеціалізованих БПЛА, які за рахунок кількості перенавантажуватимуть будь-яку систему ППО. Втрати таких БПЛА легко заповнити, а пілотам ВПС не доведеться ризикувати життям, підставляючись під вогонь зенітних ракетних комплексів, як показав досвід ведення бойових дій в Нагорному Карабаху з боку Збройних Сил Азербайджану.

Ще одна реалізація концепції мозаїчної війни є переведення функціональних можливостей, таких як радіолокація, управління вогнем та ракетами, які колись повинні були розміщуватися на загальній платформі, як складний бойовий літак, тепер можуть бути розбиті на найдрібніші практичні елементи. У концепції мозаїки, платформи «розкладаються» на свої найменші практичні функції, створюючи спільні «вузли» в єдиному інформаційному

просторі, які відрізняються високою стійкістю і можуть залишатись оперативно ефективними, навіть якщо противник знищить деякі елементи мережі.

Інший аспект мозаїчної війни, який виникає в результаті побудови дезагregованої платформи, полягає в тому, що кожен «вузол», оскільки він настільки спеціалізований, може бути набагато легшим і доступнішим, ніж великі вузькоспеціалізовані, багатовартісні бойові платформи. Дезагregовані платформи, навіть ті, що мають розширені можливості, будуть більш доступними і їх можна розробити у більшій кількості, ніж високопродуктивні платформи. Зменшення кількості датчиків на майбутніх платформах може допомогти зменшити їх розмір, вагу, складність та загальну вартість одиниці. Тому дані світові тенденції вимагають нових підходів щодо розробки озброєння та військової техніки.

Розробка системи керування групою безпілотних літальних апаратів.

Створення унікальної системи керування групою БПЛА (більше 3-ох одиниць) одним оператором в реальному масштабі часу. Ідея полягає у застосуванні невеликих ударних, розвідувальних та дронів ретрансляторів нового покоління, які здатні виконувати десятки місій у автономному режимі, використовуючи тактику «рою». Дана система передбачає створення двох основних сегментів – це система пуску та збору невеликих БпЛА та система управління роботою рою невеликих розмірів. Після виконання поставлених завдань – розвідки, дій в рамках електронної війни, скидання бойових зарядів – рой БпЛА повертається в місце зльоту або збирається іншим літаком.

Такі невеликі БПЛА здатні самостійно – без постійного контролю зі сторони оператора – виконувати декілька десятків місій, таких як сенсорні функції, ціленаведення, транспортування зброї та радіоелектронна боротьба. Це дозволить одному оператору управляти одразу багатьма такими БПЛА, в майбутньому один фахівець зможе здійснювати управління роєм невеликих літаючих роботів. Ведеться робота щодо синтезу нейронечіткої багатовимірної системи управління польотом рою БПЛА тактичного класу за умови знаходження компромісу між якістю та робастністю цієї системи. Як робастний прототип, який використовується для навчання нейронечіткої системи, застосовується автопілот, синтезований за допомогою теореми розділення з наступною робастизацією отриманого рішення на основі робастної - оптимізації. Зміни вхідних та вихідних координат чіткої системи використовуються для навчання нейронечіткої мережі, яка застосовується для алгоритму зворотного розповсюдження похибки для налаштування параметрів функцій приналежності вхідних сигналів та градієнтної оптимізації для налаштування параметрів алгоритму дефазифікації.

Сегмент розвідувальної сенсорної MESH-мережі військового призначення

Визначальною умовою досягнення стратегічної та оперативно-тактичної переваги над супротивником в ході бойових дій є високий рівень забезпечення військ (сил) всіма видами оперативної інформації. В умовах високої динаміки ведення бойових дій таку перевагу можливо досягти тільки у випадку, коли оперативна інформація про поточну обстановку доступна для всіх ланок управління (включаючи окремих військовослужбовців).

На даний час ведеться інтенсивна робота по створенню єдиного інформаційного поля для обміну інформації на різних ланках військового управління елементом якого будуть безпроводні сенсорні мережі тактичної ланки, що забезпечуватимуть прийом і передачу розвідувальної інформації про супротивника та видачу її органам управління військами та зброєю (рис.1). Загальна ідея функціонування БСМ полягає у використанні великої кількості неоднорідних безпроводових сенсорів, які можуть бути розташовані на значних географічних територіях для моніторингу за цілями або різнорідних параметрів навколишнього середовища (в деяких випадках побудови радіонапряму (ів) при знищенні основної опорної мережі зв'язку). Отримана безпроводовим сенсорним вузлом інформація передається на спеціальні шлюзи безпосередньо, або шляхом ретрансляції через проміжні сенсорні вузли. У випадку, якщо площі території для моніторингу дуже великі, у якості шлюзів можуть використовуватися сенсорні вузли на базі безпілотних літальних апаратів (БПЛА) чи аероплатформ (АП).

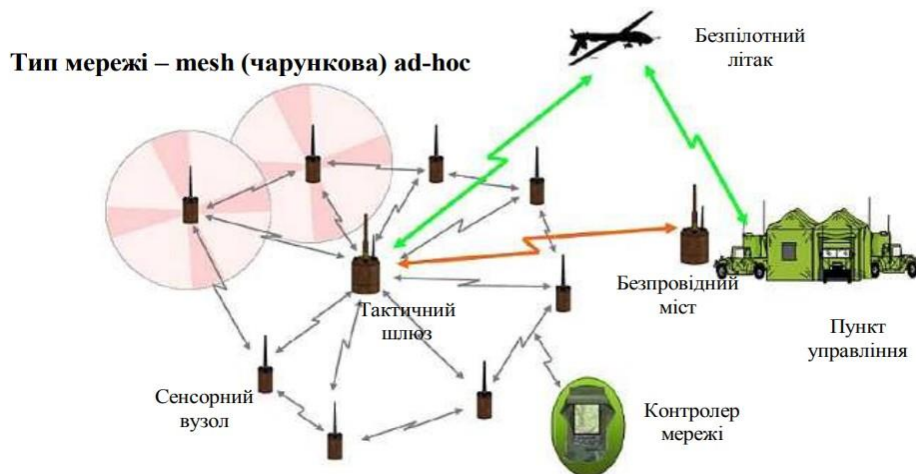


Рис.1. Типова структура безпроводної сенсорної мережу військового призначення

Використання складних ортогональних сигнально-кодових конструкцій при побудові завадозахищених каналів управління тактичних БПЛА

Як показує сучасний рівень розвитку безпілотних авіаційних комплексів (БПАК) та засобів боротьби з ними, одним з важливих завдань є забезпечення скритного та завадозахищеного керування тактичним БПЛА, або групою БПЛА в умовах роботи засобів радіорозвідки та постановки навмисних завад противником.

Даний підхід, що використовує внутрішньоімпульсну лінійну частотну модуляцію (ВЛЧМ), знайшов своє широке застосування в бездротових сенсорних мережах військового призначення та є потенційно можливим при проектуванні та створенні завадозахищеного каналу управління тактичним БПЛА за рахунок своїх високих енергетичних показників. Високі енергетичні показники дозволяють реалізувати детектування приймачем наявності корисного сигналу в просторі з низьким відношенням потужності сигналу до потужності завади в широкій смузі частот, що відкриває можливість передавати команди управління тактичним БПЛА на значні відстані при низьких потужностях випромінювання передавачем в умовах роботи засобів радіорозвідки та постановки навмисних завад противником.

Канали управління, утворені з використанням ВЛЧМ сигналів, є актуальними лише для тактичних БПЛА з відстанями між БПЛА та наземною станцією керування (НСК) лише до декількох десятків кілометрів.

Алгоритм побудови маршруту розвідувального робототехнічного комплексу в умовах невизначеності з використанням штучного інтелекту

Для вирішення задачі з проведення розвідувальної операції з використання робототехнічних комплексів (РТК) на місцевості з щільною забудовою запропоновано розглядати площину військових дій, як багатовимірний лабіринт.

Запропоновано алгоритм вирішення завдання РТК з побудови оптимального маршруту в багатовимірному лабіринті в умовах невизначеності з використанням штучного інтелекту. Перетворення, що використані при синтезі нейронної мережі носить неформальний характер, а в результаті перетворення формується структура нейронної мережі, яка в подальшому може бути навчена традиційним способом або за допомогою розрахунку значень коефіцієнтів. Запропонована структура нейронної мережі дозволяє вирішити задачу пошуку шляху виходу з лабіринту при постановці завдання, в якій на вхід нейронної мережі надходить тільки ознака успішного (або неуспішного) виконання минулої дії. Найпростіша ситуаційна модель поведінки агентів є статичною і будується на основі "ситуація-дія". Такий алгоритм створює систему планування поведінки штучного інтелекту з доповненням механізму контролю ситуації. Запропонована формальна схема побудови математичних моделей процесів ситуаційного керування і планування дій інтелектуальних агентів.

ПОБУДОВА ТРАНСПОРТНОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ЗБРОЙНИХ СИЛ УКРАЇНИ З УРАХУВАННЯМ РЕКОМЕНДАЦІЙ МІЖНАРОДНОГО СОЮЗУ ЕЛЕКТРОЗВ'ЯЗКУ ITU

Актуальність. На сьогоднішній день система військового зв'язку та автоматизації це складна, ієрархічна, розподілена система до складу якої входять інформаційно-телекомунікаційні системи різних ланок управління всіх видів Збройних Сил. Велика частка елементів системи військового зв'язку та автоматизації не сумісні між собою, так як історично будувались та модернізувались відокремлено, в межах зони відповідальності певного командування.

Однією із ключових частин системи військового зв'язку та автоматизації є її стаціонарний компонент, що забезпечує управління силами, зброєю як в мирний час так і під час приведення у вищі ступені бойової готовності, веденні операцій (бойових дій). При побудові стаціонарного компонента використовуються як власні мережеві ресурси МОУ так і мережеві ресурси орендовані в Укртелеком, *DataGroup*, ДСТЗІ. Як наслідок, ці мережі ресурси неоднорідні: це мережеве обладнання різних фірм виробників; різної технологічної основи; різних методів комутації та сигналізації; різні мережеві протоколи.

Необхідно відмітити, що в існуючих стандартах військова телекомунікаційна система виділяє тільки два рівні це: військові телекомунікаційні мережі доступу та військова транспортна телекомунікаційна мережа.

Сучасний етап розвитку стаціонарного компоненту системи військового зв'язку вказує на те, що до його складу входять: різномірні телекомунікаційні мережі військового призначення, які побудовані на обладнанні різних мережевих вендорів із власними пропрієтарними протоколами; апаратура старого парку на певних сегментах мережі; що в призводить до *не сумісності* як за протоколами передачі так і протоколами сигналізації. Особливо гостро дане питання постає при необхідності оренди каналів і трактів передачі для організації зв'язку в конкретній військовій операції. Крім того, виникає питання визначення раціонального об'єму необхідного мережевого ресурсу для обслуговування користувачів із заданими показниками якості обслуговування та організації контролю за власними інформаційними потоками в мережах різної відомчої приналежності, які використовуються для інформаційного обміну системи управління ЗСУ.

Таким чином, можливе визначити наступні основні задачі модернізації телекомунікаційної складової стаціонарного компонента системи військового зв'язку:

1. Створення загального телекомунікаційного середовища, яке забезпечить взаємодію різномірних мереж, побудованих з використанням великої кількості різномірного мережевого обладнання.
2. Забезпечення ефективного управління процесом обслуговування при використанні мережевого ресурсу із різними системами сигналізації та різними типами комутації.
3. Розробити методики, які дозволять визначити пропускну спроможність і якість обслуговування в мережах, які побудовані на базі наявного обладнання військ зв'язку Збройних Сил України.
4. Розробити методики визначення мінімально необхідного мережевого ресурсу, який потрібно орендувати в Укртелеком, *DataGroup*, ДСТЗІ, для обслуговування командування в кожній конкретній операції з заданими показниками пропускну спроможності та якості обслуговування.

Для вирішення цих питань були проаналізовані рекомендації сучасних концепцій, які розроблені міжнародним союзом електрозв'язку ITU. Перша концепція, яка була проаналізована це концепція *NGN (Next Generation Network)*.

У цих мережах рекомендоване чітке розмежування наступних рівнів (рис. 1.):

1. Рівень послуг і додатків;
2. Рівень агрегації, управління та сигналізації;
3. Рівень магістральної транспортної мережі.
4. Рівень мереж доступу.

При чому, всі рівні взаємодіють через відкриті інтерфейси.

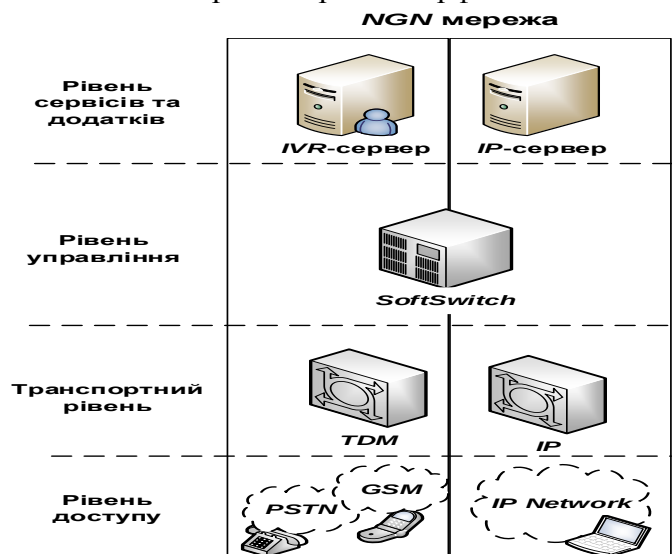


Рис. 1. Узагальнена чотирьох-рівнева архітектура NGN

Розробка концепції NGN була покликана для створення загального телекомунікаційного середовища із мереж різних технологій і різноманітного несумісного мережевого обладнання. Також одним із постулатів концепції NGN є використання стандартизованих програмних інтерфейсів *API (Application Programming Interface)*, що дозволяють об'єднувати різні інформаційні системи незалежно від обраних технологій програмної реалізації.

В результаті аналізу рекомендацій концепції NGN та їх адаптації для військової телекомунікаційної системи, була розроблена архітектура, яка представлена на рис. 2.

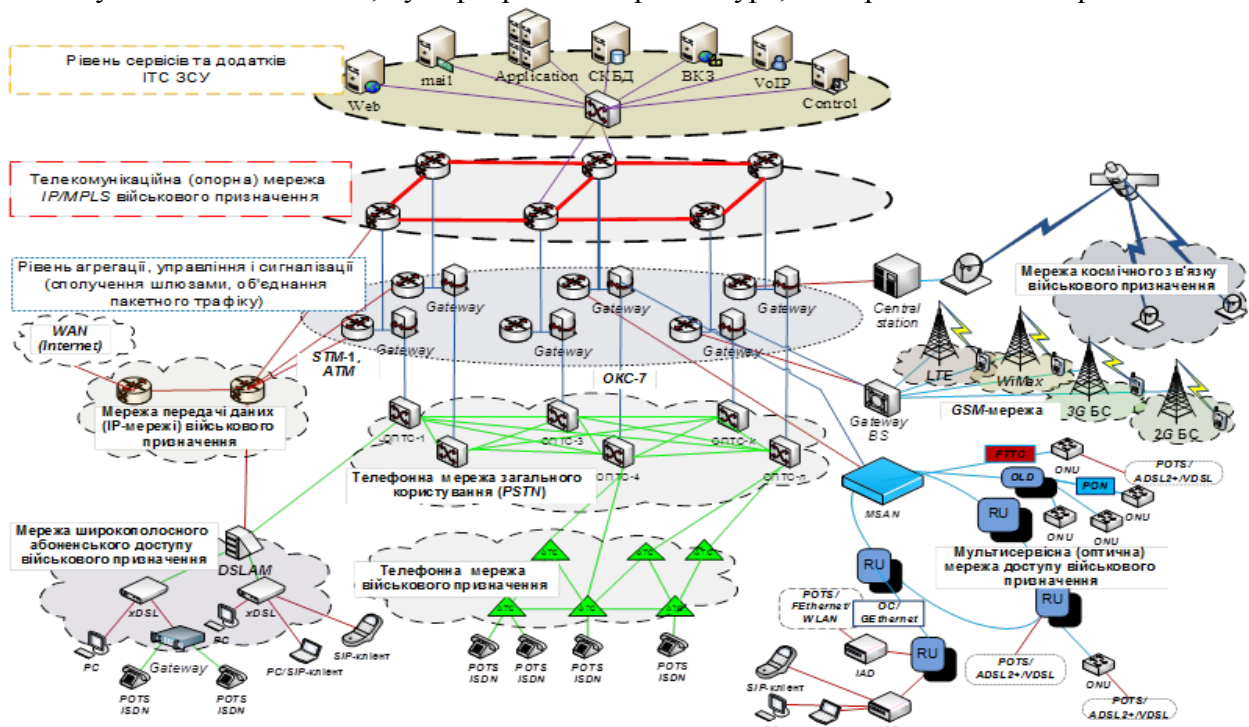


Рис. 2. Архітектура військової телекомунікаційної системи, яка відповідає вимогам NGN

Ця архітектура дозволяє провести інтеграцію різномірних військових мереж і створити загальне телекомунікаційне середовище.

Однак ці рішення прийнятні тільки коли мережі побудовані на обладнанні одного виробника. Це пов'язано з тим, що основний елемент рівня управління *SoftSwitch* різних фірм виробників не взаємодіють між собою, тобто не сумісні. В зв'язку з цим для вирішення проблеми сумісності на рівні управління були використані рекомендації наступної концепції *IMS* (*IP Multimedia Subsystem*), загальна структура якої представлена на рис. 3.

В даній концепції були використані рекомендації щодо побудови рівня управління. А саме, в *IMS* відійшли від рішення задач управління програмно-апаратними засобами (монолітними) *SoftSwitch*, а перейшли до програмно-функціональних блоків, побудова яких не залежить від фірми виробника. Необхідно відміти *IMS* дозволяє уніфікувати потоки сигналізації різних мережевих технологій та підвищити мобільність користувачів за рахунок використання протоколу *SIP*.

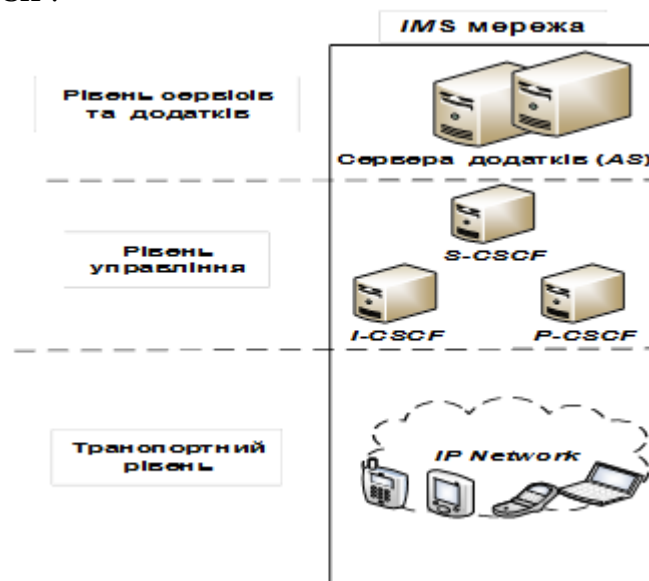


Рис. 3. Узагальнена трьох-рівнева архітектура *IMS*

Аналіз рекомендацій концепції *IMS* дозволив запропонувати архітектуру побудови рівня управління стаціонарного компонента, яка зображена на рис. 4.

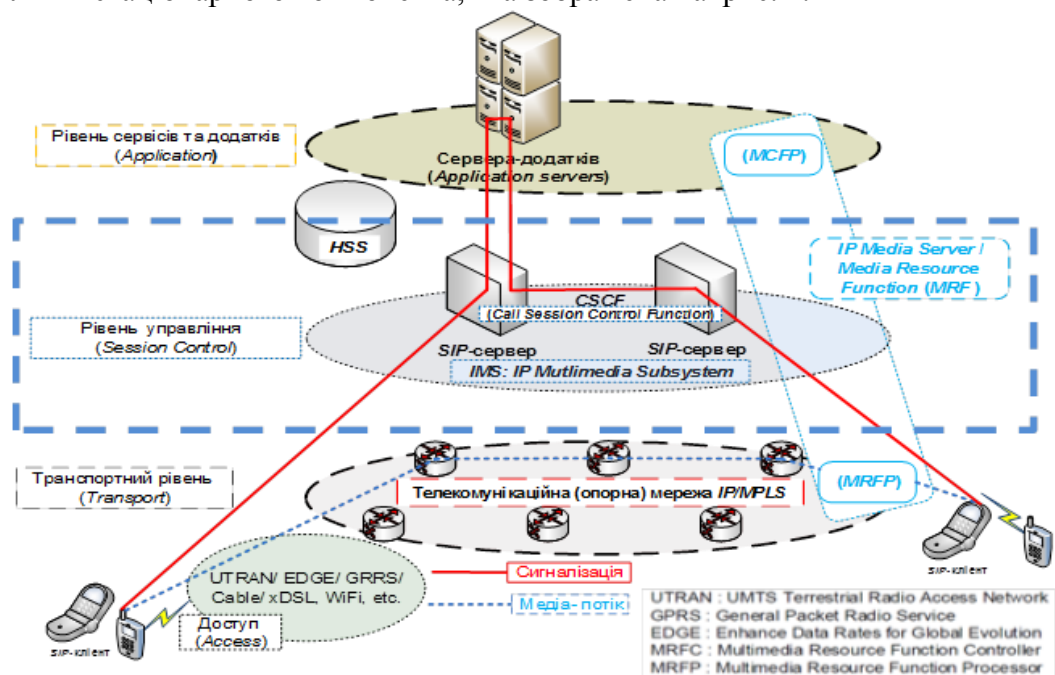


Рис. 4. Архітектура рівня управління стаціонарного компонента системи військового зв'язку з урахуванням рекомендацій концепції *IMS*

Особливістю обслуговування абонентів при передачі трафіку реального часу в такій системі полягає в тому, що одночасно виконуються два процеси:

- перший це обробка сигналізації (пошук абонентів по мережі, формування вимог щодо якості обслуговування ті інше);
- другий – виділення необхідного мережевого ресурсу для обслуговування медіа-потоків користувачів із заданою якістю.

З врахуванням недоліків існуючої військової телекомунікаційної системи та на основі переваг адаптованих концепцій *NGN* та *IMS* була синтезована архітектура стаціонарного компонента на основі мультимедійної платформи *IMS*.

Варіант побудови такої архітектури представлено на рис. 5.

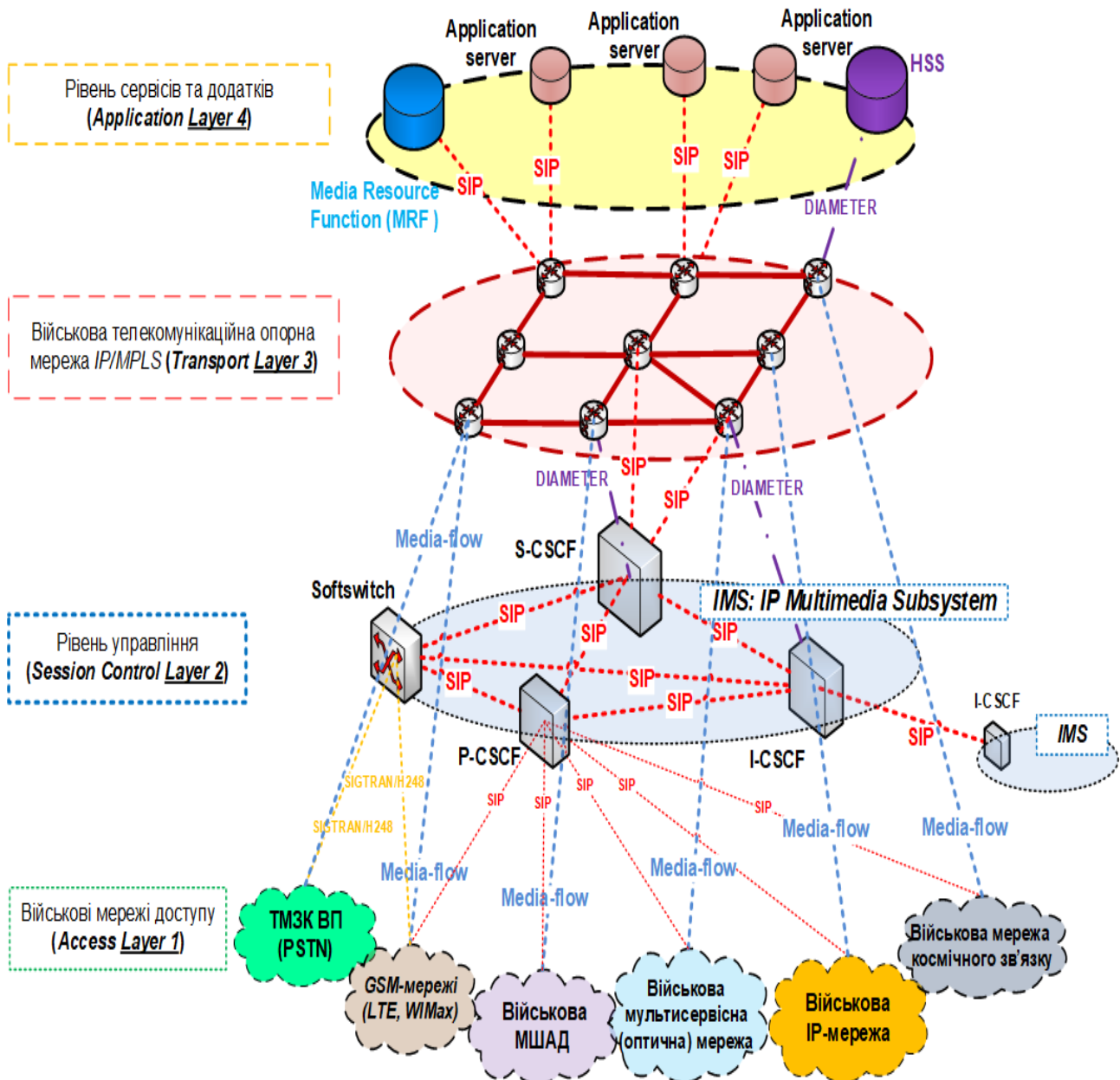


Рис. 5. Архітектура стаціонарного компонента системи зв'язку ЗСУ на основі мультимедійної платформи *IMS*

Запропонована архітектура складається із чотирьох рівнів:

1 рівень – рівень доступу, який для військових мереж складається із розгорнутих на власних засобах МОУ різномірних телекомунікаційних мереж.

2 рівень – рівень управління, який повинен будуватись на базі власного серверного обладнання МОУ та реалізувати процеси управління у відповідності з концепцією *IMS*.

3 рівень – транспортний рівень, це рівень військової телекомунікаційної опорної мережі, що складається із каналів, трактів передачі та мереж, які орендуються в Укртелеком, DataGroop, ДСТЗІ.

4 рівень – рівень сервісів та додатків на якому вирішуються прикладні задачі органів управління, а також задачі підтримки заданих показників якості обслуговування та пропускної спроможності стаціонарного компонента.

Для реалізації розробленої архітектури стаціонарного компонента на базі мультимедійної платформи *IMS* необхідно вирішити комплекс взаємопов'язаних задач:

Перша задача. Необхідно оцінити пропускну спроможність та якість обслуговування трафіку реального часу вже у розгорнутих військових телекомунікаційних мереж доступу, що відповідає першому рівню розробленої перспективної архітектури.

Друга задача. На рівні управління (другий рівень), необхідно врахувати різні типи сигналізації та додатковий об'єм трафіку сигналізації при його транскодуванні із одного типу в інший. А також визначити структуру системи сигналізації та розробити вимоги до продуктивності програмно-функціональних блоків ядра *IMS*.

Третя задача. Оцінити об'єм та кількість мережевого ресурсу, який нам потрібно орендувати в Укртелеком, DataGroop, ДСТЗІ для побудови військової телекомунікаційної опорної мережі під кожен операцію з дотримання заданих показників якості обслуговування. А це відповідає третьому рівню розробленої перспективної архітектури стаціонарного компонента.

Четверта задача. На рівні сервісів та додатків (четвертий рівень) планується розгортання системи моніторингу для контролю заданих показників якості обслуговування та реалізації методів боротьби з перевантаженнями в стаціонарному компоненті.

Для впровадження перспективної архітектури стаціонарного компонента на основі *IP Multimedia Subsystem* можуть також бути використанні сучасні інформаційні технології такі, як віртуалізація мережевих функцій *NFV (Network Functions Virtualization)*.

Використання технології віртуалізації дозволить заощадити кошти, так це дозволяє вирішувати задачі мережевого управління та надання інформаційних послуг за рахунок використання (оренди) необхідних обчислювальних потужностей в дата центрах.

Це пояснюється тим, що закупку серверного обладнання можна здійснювати у будь-якого виробника, а потім вирішувати завдання модернізації за рахунок віртуалізація мережевих функцій *NFV*. Також, використання методів віртуалізації дозволяє швидко розгортати систему управління військової телекомунікаційної системи, окремі сегменти мережі та оперативно проводити балансування навантаження в залежності від завдань, які покладаються на систему зв'язку ЗСУ.

Однак, застосування технологій віртуалізації вимагає додаткового наукового обґрунтування та опрацювання:

- визначення мережевого обладнання, яке може бути віртуалізовано;
- визначення вимог в місцях розгортання;
- визначення достатнього об'єму віртуальних ресурсів.

Висновок.

Використання запропонованих підходів при удосконаленні стаціонарного компонента системи військового зв'язку дозволяє:

1. Проводити модернізацію мережевого обладнання, сегментів військової телекомунікаційної системи окремо на різних рівнях управління не порушуючи при цьому функціонування системи в цілому (тобто поступовий перехід на *all IP*-сервіси).
2. Використовувати обладнання старого парку (або несумісне мережеве обладнання різних мережевих вендорів, що було закуплене раніше) до повної модернізації.
3. Здійснювати швидке впровадження нових мережевих технологій через стандартизовані інтерфейси.

4. Проводити інтеграцію різнорідних інформаційних систем за рахунок використання *API (Application Programming Interface)* для розробки спеціалізованого програмного забезпечення

5. Використовувати технології віртуалізації для розширення функціоналу та підвищення гнучкості, масштабованості системи управління системи зв'язку.

ЛІТЕРАТУРА

1. Гольдштейн А.Б., Гольдштейн Б.С. *SOFTSWITCH* СПб.: БХВ – Санкт-Петербург, 2006. – 368 с.: ил. ISBN 5-8206-0117-3

2. https://web.archive.org/web/20130403104827/http://www.imsforum.org/Plugfest_9

3. <https://web.archive.org/web/20130609022649/http://imsforum.org/>

4. What is the IP Multimedia Subsystem (IMS) ? <https://www.metaswitch.com/knowledge-center/reference/topic/ip-multimedia-subsystem-ims>

5. O.I. Romanov, M.M. Nesterenko, L.A. Veres. Integration Of Modern Protocols Ip-Telephony In IMS Architecture/2018 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), 10-14 Sept. 2018, Date Added to IEEE Xplore: 26 March 2020, Conference Kyiv, Ukraine.

DOI: [10.1109 / UkrMiCo43733.2018.9047587](https://doi.org/10.1109/UkrMiCo43733.2018.9047587), (e)ISBN: 978-1-5386-5264-0

6. Globa L., Skulysh M., Romanov O., Nesterenko M. (2019) Quality Control for Mobile Communication Management Services in Hybrid Environment. 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.

DOI https://doi.org/10.1007/978-3-030-16770-7_4, Print ISBN 978-3-030-16769-1

7. O.I. Romanov, M.M. Nesterenko, L.A. Veres, Hordashnyk Y.S. IMS: Model and calculation method of telecommunication network's capacity // *Proceedings of the 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, Odessa, Ukraine.

DOI: [10.1109/UkrMiCo.2017.8095412](https://doi.org/10.1109/UkrMiCo.2017.8095412), eISBN:: 978-1-5386-1056-5

АНАЛІЗ ЗАЛЕЖНОСТІ ЧАСУ ВИКОНАННЯ КРИПТОГРАФІЧНОГО ПЕРЕВОРЕННЯ ВІД ПОТУЖНОСТІ КОМП'ЮТЕРА НА ПРИКЛАДІ АЛГОРИТМУ ЦИФРОВОГО ПІДПISУ PICNIC

Важливою особливістю постквантового періоду у криптографії є суттєва невизначеність щодо вихідних даних для криптоаналізу та протидії в частині можливостей квантових комп'ютерів, їх математичного та програмного забезпечень, а також застосування квантового криптоаналізу до існуючих криптоперетворень та криптопротоколів. В якості основних методів обрано математичні методи цифрового підпису (ЦП), що пройшли суттєвий аналіз та обґрунтування в процесі широких досліджень криптографами та математиками на найвищому рівні. Вони детально описані та пройшли дослідження на 1-му етапі міжнародного конкурсу NIST США. В процесі 2-го етапу прийнято ряд рішень стосовно об'єднання деяких кандидатів на постквантовий стандарт ЦП [6].

Для подальших досліджень на 2-му етапі залишили 9 кандидатів: CRYSTALS-DILITHIUM, FALCON, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow та SPHINCS+. Три з них (Dilithium, FALCON, qTeSLA) засновані на стійкості алгебраїчних решіток (Lattice-based), чотири (GeMSS, LUOV, MQDSS, Rainbow) – на основі багатовимірних перетворень (MQ-перетворення), один (SPHINCS+) – на стійкості геш-функції, один (Picnic) – на стійкості геш-функції та блокових поточкових шифрів [4]. За результатами досліджень перспективних постквантових криптографічних алгоритмів типу цифровий підпис протягом 2-го раунду конкурсу NIST США, було отримано наступні результати – були обрані алгоритми-фіналісти та альтернативні алгоритми. У якості алгоритмів-фіналістів були обрані такі алгоритми ЦП як CRYSTALS-DILITHIUM, FALCON та Rainbow. У якості альтернативних алгоритмів – GeMSS, Picnic та SPHINCS+ [7].

Далі більш детально розглянемо перспективний постквантовий алгоритм ЦП, що входить до переліку альтернативних алгоритмів – Picnic.

Метою доповіді є викладення основних теоретичних відомостей щодо алгоритму ЦП Picnic та практична демонстрація залежності швидкості виконання як алгоритму ЦП Picnic в цілому, так і швидкості кожної з його операцій, таких як генерація ключів, операція підписання, операція перевірки, серіалізація та десеріалізація підпису. А також доведення за допомогою проведення тестів того, що швидкість виконання алгоритму ЦП не залежить від розміру повідомлення. Алгоритм ЦП Picnic – це схема підпису, яка не використовує теоретико-числові або структуровані припущення складності. Зменшення безпеки відносяться до геш-функцій і симетричних блокових шифрів. Підпис Picnic базується на неінтерактивному нульовому доказі знання секретного ключа. Підписується відкритий текст таким чином (через гешування), що тільки власник секретного ключа може вивести доказ і перевірити текст на правильність. Алгоритм ЦП Picnic має невеликий розмір відкритого ключа, але великі підписи. Підпис як і перевірка підписаного тексту досить повільні. Генерація ключів досить ефективна. Довжина підпису залежить від мультиплікативної складності схеми шифрування і від конкретної методики побудови доказу нульового знання (з області безпечних багатоваріантних обчислень). Picnic має модульну схему проектування. Криптографічні примітиви – геш-функції та блоковий шифр – можуть бути створені різними способами. Представлена конструкція використовує LowMC, блоковий шифр з низькою мультиплікативною складністю. LowMC не вивчався так багато, як AES, і, отже, потребує набагато більшого аналізу. Ефект використання AES замість LowMC в Picnic полягає в розширенні довжини підпису на коефіцієнт, який коливається від 6 до 9, в залежності від розміру блоку. Покращення обчислень призведе до зменшення підписів. Варто зазначити, що вимоги безпеки для базового блочного шифру менш строгі, ніж загальні вимоги безпеки до блокового шифру, тому що тільки одна (випадковий відкритий текст, шифртекст) пара коли-

небудь розкривається [2]. Відкритим ключем для шифру є пара (C, p) , де $C=E(sk, p)$, а E – блоковий шифр, sk – секретний ключ, а p – блок відкритого тексту. Блоковий шифр E – LowMC. Для виготовлення підпису підписувач має створити неінтерактивний доказ знань sk і пов'язати доказ з повідомленням, яке збирається підписати. Було обрано LowMC, бо він забезпечує менший розмір підпису, ніж можливі альтернативні варіанти.

Доказом знання є спеціалізована версія ZKBoo – ZKB++. Ця система доказу працює наступним чином: той, хто має підтвердити себе, імітує протокол конфіденційного обчислення (MCP протокол), який дозволяє сторонам спільно перевірити, що $E(sk, p)=C$, якщо кожна зі сторін має частку sk . Кількість учасників цієї операції є параметром для шифру. Ідея полягає в тому, щоб змусити того, хто доводить, прийняти модельований стан та стеганограми всіх сторін, після цього дозволити підтверджувачу відкрити випадкову підмножину модельованих сторін, побачивши їх завершений стан. Потім він перевіряє, чи правильно проведено обчислення з точки зору відкритих сторін, і якщо так, він може бути впевненим у тому, що результат правильний. Протокол MPC гарантує, що відкриття підмножини сторін не розкриває інформацію про секрет. Повторне паралельне виконання цього процесу дає високу впевненість у тому, що той, хто доводить, знає таємницю [2, 3].

Щоб зробити доказ не інтерактивним, використовується два варіанти. Перетворення Fiat-Shamir (FS) дає схему підпису, захищену у ROM (random oracle model), тоді як перетворення Unruh (UR) дає схему підпису, захищену у QROM (quantum random oracle model) [2, 3]. Picnic має три рівні безпеки L1, L3 і L5, кожен з яких відповідає вимогам AES-128, AES-192 і AES-256 безпеки відповідно. Для кожного рівня безпеки існує два алгоритми підпису: FS і UR. FS – на основі перетворення Fiat-Shamir – включає в себе: picnic-L1-FS, picnic-L3-FS та picnic-L5-FS. UR – заснований на перетворенні Unruh – включає в себе: picnic-L1-UR, picnic-L3-UR та picnic-L5-UR. Picnic2 виконується тільки за допомогою перетворення Fiat-Shamir. Є також три рівні безпеки для Picnic2: picnic2-L1-FS, picnic2-L3-FS та picnic2-L5-FS. Всі параметри для кожного рівня вибираються так, щоб вони, як очікується, забезпечували, щонайменше, $S/2$ біт захисту від атак на квантових комп'ютерах і S біт захисту від атак, що реалізовані класичними комп'ютерами.

Слід звернути увагу на криптографічні компоненти алгоритму, а саме: сімейство блокових шифрів LowMC, геш-функції, криптографічні функції формування ключа (KDF) [2, 3].

LowMC. Підписання та перевірка обчислюють LowMC цикл як частину неінтерактивного моделювання протоколу MPC. Алгоритми підписання та перевірки, визначені в даному шифрі, містять достатню умову для використання LowMC. Наступні параметри є різними для кожного з трьох наборів параметрів LowMC (L1, L3, L5): $Kmatrix$ – масив $n \times n$ двійкових матриць, одна для початкового зачищення, інша для кожного раунду LowMC ($r+1$ загалом). $Lmatrix$ – масив $n \times n$ двійкових матриць, по одній для кожного раунду LowMC (r загалом). $roundconstant$ – масив n -бітних векторів, по одному для кожного раунду LowMC [2, 3].

Геш-функції. Усі геш-функції алгоритму засновані на функціях SHAKE128 або SHAKE256 SHA-3, які мають змінну вихідну довжину. Ці функції для шарів Picnic2 наведені в таблиці 1, із заданою довжиною виходу, також вказаною в таблиці 1. Існує кілька операцій гешування при обчисленні підписів, перший раз для обчислення зобов'язань, другий раз – для перевірки (необов'язково), при обчисленні другого типу передачі і при використанні початкового значення в декількох місцях. До входу H додається фіксований байт, щоб визначити геш-входи в різних режимах. Визначення відбувається наступним чином $H_i(x)=H(0x0ikx)$, для $i=0,...,5$. При обчисленні зобов'язань ми використовуємо H_0 , а при обчисленні перевірки – H_1 . Набори параметрів UR також використовують H при обчисленні функції з використанням H_2 . Перед кожним використанням початкового значення, яке використовується в декількох місцях, гешуємо його за допомогою H_2 , H_4 або H_5 [2, 3].

Криптографічні функції виведення ключа (KDF). Створюючи та перевіряючи підписи, ми маємо розширювати коротке випадкове значення, яке називається початковим, з 128–512

біт до близько 1 КБ. Це робиться за допомогою функції розширюваного виводу (XOF) на основі SHA3, що називається SHAKE. Це дозволяє використовувати одне сімейство функцій (SHA3) як для гешування, так і для формування ключів, оскільки SHAKE з заданою довжиною виходу також є безпечною геш-функцією. На рівні безпеки L1 використовується функція SHAKE128, а на рівні безпеки L3 та L5 – SHAKE256. Додаткові значення, такі як контекст, мітка та вихідна довжина, повинні кодуватися і передаватися XOF як єдина вхідна комбінація [2, 3]. Процес генерації однаковий для всіх наборів параметрів. Відкритий ключ позначається $pk=(C, p)$, а особистий ключ – sk . Вхід для генерації ключів – рівень безпеки (один із $S=128, 192$ або 256). Зверніть увагу, що ключову пару рівня безпеки S технічно можливо використовувати з усіма алгоритмами підпису, визначеними на цьому рівні, наприклад, пара ключів, створена за допомогою 128-бітного набору параметрів, може використовуватися для $picnic-L1-FS$ та $picnic-L1-UR$. Не рекомендується використовувати ключову пару з декількома алгоритмами підпису. Алгоритм генерації ключа складається з трьох етапів [2, 3]:

1. Виберіть випадковий n -бітовий рядок p та випадковий n -бітовий рядок sk .

2. Обчисліть шифрування p за допомогою sk , визначеного як $C=E(sk, p)$ за допомогою LowMC з параметрами.

3. На виході отримуємо пару (sk, pk) . Секретний ключ – sk і відкритий ключ $pk = (C, p)$.

Після створення ключа починається операція підпису:

Вхід: пара ключів підписувача (sk, pk) , повідомлення, яке має бути підписано масивом байтів M , таким чином, що $1 \leq M \leq 2^{55}$.

Вихід: Підпис на M у вигляді масиву байтів.

Операція перевірки після операції підписання:

Вхід: відкритий ключ pk підписуючого, повідомлення у вигляді масиву байтів M , таке, що $1 \leq M \leq 2^{55}$, підпис σ (також масив байтів).

Вихід: дійсний, якщо σ є підписом M щодо pk або недійсний, якщо ні.

Серіалізація і десеріалізація (S і D) [2, 3]. Відкритий ключ шифрування (C, p) повинен бути серіалізований як біти C , за якими слідує біт p . Обидва спершу перетворені в байтові масиви, обидва довжиною S біт, а S повинно бути гарантовано кратним восьми. Тому для заданого набору параметрів відкриті ключі можуть бути однозначно проаналізовані. Довжина серіалізованого відкритого ключа однозначно визначає рівень безпеки, але не точний набір параметрів, наприклад, відкриті ключі як для $Picnic-L1-FS$, так і для $Picnic-L1-UR$ мають однакову довжину. Програми, які обробляють кілька наборів параметрів, відповідають за кодування набору параметрів разом із відкритим ключем. Серіалізація особистого ключа здійснюється серіалізацією S бітів sk , як масиву байтів. Як і у випадку відкритого ключа, довжина особистого ключа визначає рівень безпеки, але не набір параметрів. Програми, що працюють з особистими ключами для декількох наборів параметрів, також повинні серіалізувати набір параметрів.

S:

Вхід: Підпис $(e, salt, b_0, \dots, b_{T-1}, z_0, \dots, z_{T-1})$;

Вихід: масив байтів B , кодуючий підпис.

D:

Вхід: масив байтів B , кодуючий підпис.

Вихід: Підпис $(e, salt, b_0, \dots, b_{T-1}, z_0, \dots, z_{T-1})$ або $null$ у разі невдачі десеріалізації.

Виконання підписів $Picnic$ слабо залежить від довжини повідомлення, яке потрібно підписати. Далі використовується 500 байтове повідомлення для кожного рівня безпеки і налаштувань $Picnic$. В таблиці 1 наведені параметри для трьох рівнів безпеки L1, L3 і L5, що відповідають безпеці AES-128, AES-192 і AES-256 (відповідно). Для кожного з трьох рівнів безпеки існує два алгоритми підпису які використовують систему перевірки ZKB, засновану на перетворенні Fiat Shamir (FS): $picnic-L1-FS$, $picnic-L3-FS$ і $picnic-L5-FS$, й засновану на перетворенні Unruh (UR): $picnic-L1-UR$, $picnic-L3-UR$ і $picnic-L5-UR$. Існує також три набори налаштувань, що використовують перетворення FS і систему підтвердження з алгоритму

покращення неінтерактивних нульових знань за допомогою додатків для постквантових підписів [2].

Таблиця 1

Параметри рівнів безпеки								
Набір параметрів	S	n	s	r	Hash/KDF	L_h	T	u
picnic-L1-FS	128	128	10	20	SHAKE128	256	219	-
picnic-L1-UR							219	-
picnic2-L1-FS							343	27
picnic-L3-FS	192	192	10	30	SHAKE256	384	329	-
picnic-L3-UR							329	-
picnic2-L3-FS							570	39
picnic-L5-FS	256	256	10	38	SHAKE256	512	438	-
picnic-L5-UR							438	-
picnic2-L5-FS							803	50

Всі параметри обрані так, що очікується, що вони забезпечать S біт безпеки від класичних атак, і як мінімум $S/2$ біт безпеки від квантових атак [2]. Параметр u , кількість спірних повторень, застосовано лише до наборів параметрів picnic2. Параметр N , кількість сторін в імітації MPC завжди 64 для наборів параметрів picnic2 [2, 3].

Таблиця 2

Розмір ключа і підпису (в байтах) за рівнем безпеки				
Набір параметрів	Відкритий ключ	Секретний ключ	Підпис (макс.)	Підпис (сер., відх.)
picnic-L1-FS	32	16	34016	32838, 107
picnic-L1-UR			53945	-
picnic2-L1-FS			13786	12359, 213
picnic-L3-FS	48	24	76764	74134, 198
picnic-L3-UR			121837	-
picnic2-L3-FS			29742	27173, 443
picnic-L5-FS	56	32	132856	128176, 315
picnic-L5-UR			209506	-
picnic2-L5-FS			54732	46282, 613

Для варіантів FS довжина підпису змінюється в залежності від виклику, тому вказується максимально можливий розмір разом із середнім розміром і стандартним відхиленням, що обчислюється за 100 підписами [3].

Результати досліджень. Основною метою було тестування часу кожної окремої операції алгоритму ЦП для різних довжин повідомлень на різних пристроях з різними характеристиками. Всі тести проводилися в однакових умовах і з використанням однієї і тієї ж операційної системи. Характеристики апаратних засобів та ОЗП усіх комп'ютерів для тестування наведено у таблиці 3.

Таблиця 3

Характеристики використовуваних ПК	
ПК1	
ОС	Linux Ubuntu 18.04
Центральний процесор	Intel Core i5-6200U @ 2.30 – 2.80 GHz (2 Cores)
Графічний процесор	NVIDIA GeForce 940M
ОЗП	6.00GB DDR3 @ 1600 MHz
ПК2	
ОС	Linux Ubuntu 18.04
Центральний процесор	Intel Core i5-7200U @ 2.50 – 3.10 GHz (2 Cores)
Графічний процесор	NVIDIA GeForce 940MX
ОЗП	8.00GB DDR4 @ 2133 MHz
ПК3	
ОС	Linux Ubuntu 18.04
Центральний процесор	AMD Ryzen 7 3750H @ 2.30 – 4.00 GHz (4 Cores)
Графічний процесор	NVIDIA GeForce RTX 2060
ОЗП	16.00GB DDR4 @ 2400 MHz

Таблиця 4

Результати тестів на ПК1

Налаштування Picnic	Довжина (байти)	Час генерації (мс)	Час підпису (мс)	Час перевірки (мс)	Час тестування відкритого ключа (мс)	Час тестування секретного ключа (мс)	Загальний час (мс)
Picnic_L1_FS	32681/34032	149	66192	44220	44981	73	155773
Picnic_L1_UR	53961/53961	236	77340	53024	53506	77	184313
Picnic_L3_FS	73734/76772	313	222537	150868	148669	179	522733
Picnic_L3_UR	121845/121845	284	251325	175741	173250	169	600925
Picnic_L5_FS	127516/132856	497	550174	366928	368993	371	1287125
Picnic_L5_UR	209506/209506	443	601042	398129	401610	352	1544601
Picnic2_L1_FS	12019/13802	177	1792100	988269	1017214	78	3797989
Picnic2_L3_FS	27617/29750	289	5509339	2804805	2829177	200	11143938
Picnic2_L5_FS	45011/54732	483	12621985	6184002	6177838	391	24984842

Таблиця 5

Результати тестів на ПК2

Налаштування Picnic	Довжина (байти)	Час генерації (мс)	Час підпису (мс)	Час перевірки (мс)	Час тестування відкритого ключа (мс)	Час тестування секретного ключа (мс)	Загальний час (мс)
Picnic_L1_FS	32784/34032	167	59122	38646	37800	65	135977
Picnic_L1_UR	53961/53961	166	66459	45018	45771	63	157630
Picnic_L3_FS	74276/76772	278	187046	126783	125560	155	440086
Picnic_L3_UR	121845/121845	238	214628	149605	148556	162	513347
Picnic_L5_FS	128024/132856	445	467341	319282	316294	309	1103851
Picnic_L5_UR	209506/209506	391	507295	349940	343942	308	1202054
Picnic2_L1_FS	12206/13802	161	1563289	846955	841369	60	3251961
Picnic2_L3_FS	27321/29750	254	4702859	2412332	2400065	168	9515814
Picnic2_L5_FS	46180/54732	420	10837245	5230015	5230015	333	21300388

Таблиця 6

Результати тестів на ПК3

Налаштування Picnic	Довжина (байти)	Час генерації (мс)	Час підпису (мс)	Час перевірки (мс)	Час тестування відкритого ключа (мс)	Час тестування секретного ключа (мс)	Загальний час (мс)
Picnic_L1_FS	32800/34032	183	32266	21535	21304	35	75922
Picnic_L1_UR	53961/53961	116	41482	25923	27020	36	94913
Picnic_L3_FS	73988/76772	268	122490	79615	84323	107	287183
Picnic_L3_UR	121845/121845	163	156229	99424	99068	88	355295
Picnic_L5_FS	128248/132856	465	320699	220257	213088	203	755190
Picnic_L5_UR	209506/209506	264	354157	248016	244950	221	848048
Picnic2_L1_FS	12398/13802	114	851125	479660	487082	37	1818445
Picnic2_L3_FS	27465/29750	175	2851473	1486124	1446177	101	5784419
Picnic2_L5_FS	46613/54732	263	7030765	3557832	3461615	201	14051176

ВИСНОВКИ

На конкурс NIST США щодо стандарту ЦП було подано механізм ЕП, що ґрунтується на стійкості геш-функції та блокових потокових шифрів – Picnic. Наразі він досліджується на 3-му етапі конкурсу NIST США у якості альтернативного алгоритму. Побудова ЦП в

алгоритмі Picnic заснована на перетворенні Fiat-Shamir (FS) та перетворенні Unruh (UR). Оцінка параметрів алгоритму говорить про те, що сам алгоритм досить збалансований за усіма критеріями, але має великий розмір підпису. Спроби зменшення розміру підпису призводять до зменшення безпеки алгоритму. Великою перевагою алгоритму є великий простір для покращення та змін, які постійно проводяться, та коли буде представлена кінцева версія алгоритму, його можна затверджувати для застосування.

Після експериментального дослідження швидкодії різних етапів алгоритму на різних персональних комп'ютерах можна сказати, що кожен з етапів безпосередньо залежить від обчислювальних здібностей комп'ютера, і зокрема, центрального процесора та ОЗП. Чим вище частота процесора і ОЗП, тим швидше буде шифруватися повідомлення. Графічний процесор практично не впливає на продуктивність. Отже можна сказати, що швидкість виконання алгоритму не залежить від довжини повідомлення (для відносно невеликих повідомлень).

ЛІТЕРАТУРА

1. Daniel Kales Efficient FPGA Implementations of LowMC and Picnic / Daniel Kales, Sebastian Ramacher, Christian Rechberger, Roman Walch, Mario Werner // . – Режим доступу: <https://eprint.iacr.org/2019/1368.pdf>.
2. Melissa Chase The Picnic Signature Scheme. Design Document / Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, Greg Zaverucha // . November 29, 2017. Version 1.0. [Електронний ресурс]. – Режим доступу: <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions>.
3. Melissa Chase The Picnic Signature Scheme. Design Document / Melissa Chase, David Derler, Steven Goldfeder, Jonathan Katz, Vladimir Kolesnikov, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, Xiao Wang, Greg Zaverucha // . March 30, 2019. Version 2.0. [Електронний ресурс]. – Режим доступу: <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions>.
4. NIST submissions. Picnic. Picnic-FS. Picnic-UR. Non-interactive Proof of Knowledge. [Електронний ресурс]. – Режим доступу: <https://pqc-wiki.fau.edu/w/Special:DatabaseHome>.
5. Itai Dinur The Picnic Post-Quantum Signature Scheme and its Security Analysis. – Режим доступу: <https://www.cs.technion.ac.il/~biham/Workshops/Cryptoday/2018/Slides/cryptoday-2018-itai-dinur-picnic.pdf>.
6. Горбенко І. Д. Методи, методика та результати порівняльного аналізу кандидатів на постквантовий стандарт електронного підпису / І. Д. Горбенко, О. Г. Качко, М. В. Єсіна, В. А. Пономар // XX Ювілейна Міжнародна науково-практична конференція "Безпека інформації в інформаційно-телекомунікаційних системах", 22 – 24 травня, 2018, м. Буча. – С. 96 – 97.
7. Gorbenko I. Electronic signature mechanisms. The Current State, the Existing Contradictions and Prospects of Practical Use for the Post-Quantum Period / I. Gorbenko, A. Kuznetsov, Yu. Gorbenko, S. Kavun, O. Kachko, M. Yesina // . ASC Academic Publishing Minden, Nevada, USA, 2017 – 165 p.

МОДЕЛЬ ВІДМОВОСТІЙКОГО СХОВИЩА ДАНИХ НА БАЗІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ Ceph

Сьогодні загальнодоступні, приватні та гібридні хмарні моделі є домінуючими стратегіями для цілей забезпечення масивної інфраструктури, і програмне забезпечення Ceph стає популярним у відповідних рішеннях хмарних систем зберігання даних. Хмари розраховують на загально вживані апаратні засоби і дане програмне рішення найкращим чином підходить для ринкових апаратних засобів для надання відмовостійких і високонадійних системи зберігання корпоративного рівня, а також для ЗС України з сторони вартості та безпеки збереження даних на власних серверних системах. Ceph відповідає даним вимогам та є досить легким у адмініструванні а також дає можливість здійснювати реплікацію даних, тобто файли будуть зберігатися на всіх вузлах кластеру та у разі відмови одного з вузлів, всі дані будуть знаходитись на іншому вузлі. Ceph – програмно обумовлена розподілена файлова система з відкритим вихідним кодом, позбалена вузьких місць і єдиних точок відмови разом з тим вона зберігає дані на одному розподіленому серверному кластері та забезпечує інтерфейс рівня об'єкту, блоку та файлу. Основні цілі Ceph – бути повністю розподіленим без єдиної точки відмови, масштабованим до рівня ексабайт та вільно доступним. Ceph забезпечує підприємствам велику продуктивність, необмежену масштабованість, потужність і гнучкість, разом з тим, дозволяє заощадити певну суму коштів шляхом відмови від комерційних рішень інших фірм, так як це програмне забезпечення є з відкритим вихідним кодом. Ceph є уніфікованим рішенням для зберігання даних рівня підприємства, що визначаються програмним забезпеченням, яке працює на стандартних апаратних засобах, що робить його найбільш економічно-ефективною і функціональною системою зберігання даних. Цей програмний інструментарій надає блокові, файлові і об'єктні системи зберігання в одному комплексі, що дозволяє клієнтам використовувати систему зберігання відповідно до їх завдань і потреб. На рисунку 1 схематично зображено один з варіантів реалізації відмовостійкого сховища даних з використанням програмного забезпечення Ceph, коли при виході з ладу будь-якого диска, вузла або групи вузлів Ceph забезпечить не тільки збереження даних, але й відновить втрачені копії на інших працездатних вузлах поки виведені з ладу диски або вузли не відновлять відповідні фахівці. При цьому процес відновлення втрачених даних та їх реплікація відбудеться без затримки, тобто клієнт не помітить збою в системі.

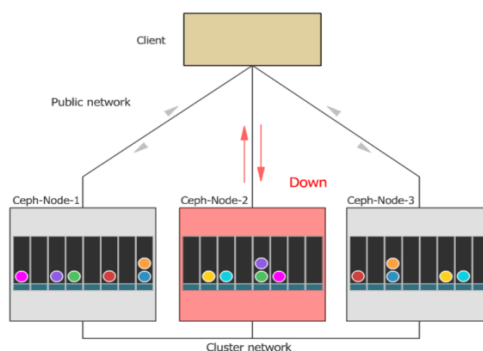


Рис.1 Варіант відмовостійкого сховища даних на базі Ceph

Отже, необхідність зберігання інформації в світі стрімко розвивається, тому необхідна система зберігання даних, яка буде масштабуватись до рівня багатьох ексабайт, і при цьому не вплине негативно на надійність зберігання даних і продуктивність. Вирішенням даних проблем є побудова систем зберігання даних з використанням даного програмного забезпечення, разом з тим Ceph користується попитом у багатьох країнах та організаціях, оскільки воно є чудовим рішенням для хмарних систем зберігання даних з підтримкою майже будь-яких хмарних платформ.

АЛГОРИТМИ МАШИННОГО НАВЧАННЯ ТА ЇХ ВИКОРИСТАННЯ У СФЕРІ КІБЕРБЕЗПЕКИ

Актуальність. Для ефективного та швидкого реагування на кіберзагрози в сучасних системах використовуються технології машинного навчання. Вони дозволяють виявляти нові загрози в інформаційних системах та спрощувати роботу аналітиків у сфері інформаційної безпеки. Машинне навчання використовується для виявлення вторгнень, аналізу шкідливих програм та удосконалювати системи реагування на кібератаки.

Мета. Проаналізувати алгоритми машинного навчання, що використовуються для виявлення кіберзагроз.

Основні положення. Методами машинного навчання (МН) зазвичай називаються такі методи побудови алгоритмів, що можуть самостійно знаходити рішення завдання, опираючись на математичні закономірності на основі яких створюються прогнози. Ціль даної технології - частково або повністю автоматизувати рішення різних складних аналітичних задач та здатне прискорити реагування на загрози в інформаційно-телекомунікаційній системі. Алгоритми МН розподіляються на методи традиційного та глибокого навчання, які потребують великого набору даних, що були попередньо проаналізовані так класифіковані для вирішення певного завдання у сфері кібербезпеки.

Щоб спроектувати ефективну систему для протидії кіберзагрозам – для кожної системи захисту необхідно розуміти всі специфічні особливості властивості вхідних даних, відповідно до яких необхідно підібрати оптимальний алгоритм.

Таблиця 1

Застосування алгоритмів машинного навчання у сфері кібербезпеки

Методи машинного навчання	Системи виявлення вторгнень	Систему аналізу шкідливих програм	Системи виявлення спаму та фішингу
Глибоке навчання	Feedforward Neural Network, Stacked Autoencoders		
	Deep Belief Network		Convolutional Neural Network
Традиційне навчання	Shared Nearest Neighbor, K-Nearest Neighbor, Logistic Regression, Random Forest, Naïve Bayes, Кластеризація, Асоціація		
	Hidden Markov Models		Support Vector Machines

В таблиці вказані сімейства алгоритмів, що використовуються для виявлення аномалій та класифікації загроз у відповідних системах кіберзахисту. Ефективність функціонування систем, в які інтегроване машинне навчання залежить від її структури, вибору вектору вхідних даних, підбору навчальної та тестової вибірок. Основні недоліки систем, в які інтегровані методи МН – необхідність постійно перенавчати системи для коректної роботи, окрім цього сучасні методи визначення на основі сигнатур не дозволяють виявити нові загрози, даних про які немає у базі системи. Для прийняття рішення, яке відбувається за нетривіальним сценарієм, необхідний додатковий аналіз спеціалістом з кібербезпеки.

Висновок. Отже, методи МН впроваджуються відповідно до їх цільового призначення. При розробці програмного забезпечення для виявлення інцидентів необхідно обробити велику кількість даних для забезпечення ефективної протидії готового інструменту на кібератаки. Інтегрування алгоритмів МН здатне покращити стійкість інформаційно-телекомунікаційної системи в цілому, забезпечити швидке визначення та реагування на кібератаки, класифікувати аномалії та передавати спеціалістам у сфері інформаційної безпеки дані у випадку неспроможності розпізнати рішення самостійно.

АНАЛІЗ МЕТОДИК ТЕСТУВАННЯ НА ПРОНИКНЕННЯ МЕРЕЖІ VPN СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Актуальність. Сучасний розвиток інформаційних технологій та необхідність розгортання мереж VPN спеціального призначення вимагає впроваджувати нові методики аналізу захищеності даних мереж. В той же час, захист має будуватися на аналізі основних вразливостей, які можливо виявити шляхом застосування методології тестування на проникнення (Penetration Testing).

Мета. Провести аналіз сучасних методик тестування на проникнення мереж, побудованих за допомогою VPN технологій, для подальшого підвищення їх захищеності.

Основні положення. Мережі VPN створюються на базі відкритих каналів загальнодоступної мережі та забезпечують з'єднання і безпечну передачу інформації вузлами зв'язку, пунктами управління та з віддаленими користувачами.

Технологія тунелювання будується на основі роботи протоколів різних рівнів, які складають основу функціонування шифруючих маршрутизаторів. Відповідно, є багато видів VPN, але найбільш розповсюдженим в мережах спеціального призначення є IPSec.

При оцінці захищеності мереж VPN використовується методологія – тестування на проникнення в ході якого використовуються прийоми і інструменти, що застосовуються зловмисниками. Завдання тестування зводиться не тільки до виявлення уразливості, яку теоретично може використовувати зловмисник, але і до експлуатації знайденої уразливості для підтвердження її реальної небезпеки.

Методологія тестування на проникнення складається з наступних етапів:

ідентифікація цілей;

пошук вразливостей;

експлуатація вразливостей;

формування протоколу (звіту) про результати тестування.

Враховуючи даний факт, пропонується наступна класифікація методів тестування на проникнення:

за розташуванням програмно-апаратних засобів та аудитора відносно периметру підрозділу (зовнішнє, внутрішнє);

за обізнаністю аудитора про цільову систему (білий ящик, чорний ящик, сірий ящик);

за обізнаністю технічних працівників підрозділу про проведення тестування (відкрите, приховане);

за характером заходів, що проводяться (пасивне, агресивне, обережне, прораховане);

за повнотою виконання тестування (повне, обмежене, фокусне);

за видом інструментів, що використовуються (з застосуванням програмно-апаратних засобів, з застосуванням методів соціальної інженерії та проникнення на контрольовану територію).

Використовуючи певну вибірку методів тестування на проникність можна сформулювати індивідуальну методику для отримання інформації про структуру мережі та виявлення її вразливостей для подальшого їх усунення та підвищення захищеності мережі VPN.

Висновок. Отже, проведений аналіз показав доцільність та перспективність застосування методик тестування на проникність при проведенні комплексної перевірки VPN та потребує подальшого дослідження.

СИСТЕМИ АНАЛІЗУ ТА УПРАВЛІННЯ ПОТОКАМИ ДАНИХ

Актуальність. В умовах сьогодення інформаційні технології розвиваються дуже стрімко, потоки даних, що генеруються, з одного боку виконують завдання ефективного інформаційного забезпечення, а з іншого несуть серйозну загрозу інформаційній безпеці. З появою ефективних автоматизованих систем управління, що на основі переліку даних здійснюють розрахунки та приймають рішення, інформація перестала бути допоміжним ресурсом. Всі процеси, починаючи з щоденних шаблонних завдань звичайного маленького підприємства і закінчуючи складними, багаторівневими завданнями управління високотехнологічним підприємством, відбуваються на основі аналізу даних. Сучасний кіберзлочинець використовує низку інструментів для здійснення впливу на потоки даних, що значно ускладнює планування та впровадження заходів інформаційної безпеки. Класичні підходи щодо аналізу та управління даними, які базуються на використанні міжмережевих екранів або їм подібних апаратно-програмних засобів дедалі більше показують свою неефективність, так як вони, по суті, просто фільтрують трафік на основі заголовку пакетів.

Виклад основного матеріалу дослідження. Існують наступні класи систем аналізу даних: на основі сигнатурного аналізу, аналізу поведінки, штучного інтелекту та гібридні. Під час дослідження розглядалися системи на основі сигнатурного аналізу.

Однією з найбільш ефективних технологій аналізу та управління даними є Deep Packed Inspection (DPI). Системи DPI здатні детально аналізувати склад пакету даних, виявляти паразитний, вірусний і „закільцьований” трафік, наявність якого збільшує навантаження на мережеве устаткування і канали зв'язку; виявляти шкідливе і несанкціоноване програмне забезпечення: мережеві сканери, троянські програми, навіть такі що розосереджені по пакетах трафіку і в такому вигляді не несуть загроз. Не менш важливою особливістю технології DPI є здатність проводити та використовувати статистичний аналіз даних (довжина пакетів даних, наявність певних символів в тілі пакету та ін.) з метою визначення пріоритетності їх обробки або алгоритму дій. Системи DPI, як правило, встановлюються в розрив існуючих з'єднань, що йдуть від граничних маршрутизаторів. Саме тому увесь потік даних, що надходить або покидає мережу проходить через DPI. Основним методом DPI систем є перевірка сигнатур протоколів та застосунків. Під сигнатурами розуміється шаблон опису даних (модель), який однозначно відповідає протоколу або застосунку. Наприклад, це може бути пошук ключових слів в даних пакету, таких як BitTorrent або запитів GET/POST протоколу HTTP. Найпростіші сигнатури ґрунтуються на URL-адресах в заголовку HTTP, їх легко створювати під конкретні цілі суб'єктів аналізу даних. Частина методів DPI систем базується на критеріях поведінки потоку даних, що дозволяє виявити сканування IP-адрес або портів. Особливості роботи систем DPI можуть значною мірою впливати на продуктивність та швидкість роботи сучасних автоматизованих систем, які генерують та обробляють значні об'єми даних, так як аналіз великих масивів даних в масштабі реального часу викликає значну затримку. Пропонований варіант використання систем DPI полягає в їх адаптації до конкретного випадку на основі розрахунку ризиків впливу на той чи інший елемент автоматизованої системи та негативних наслідків такого впливу. При вказаному підході система DPI буде працювати як система швидкого маніпулювання даними і проводити аналіз тільки пріоритетних потоків інформації, що дозволить підвищити ефективність її використання в реальному масштабі часу без втрати загальної продуктивності мережі. В даному випадку DPI систему більш доцільно розмістити „ближче” до автоматизованої системи та використовувати її в поєднанні з міжмережевим екраном, встановленим після граничного маршрутизатора мережі для базової фільтрації трафіку.

Висновок. Однією з основних переваг DPI систем на ряду з дієвим механізмом аналізу вмісту пакетів даних є гнучкість та можливість адаптації під конкретний випадок. Необхідність використання систем детального аналізу даних визначається ризиками впливу на інформаційні потоки та наслідками такого впливу.

ОСОБЛИВОСТІ СИСТЕМИ КОНТРОЛЮ ІНФОРМАЦІЙНИХ ПОТОКІВ

Актуальність. Для побудови комплексних систем захисту інформації необхідно проводити аналіз ризиків інформації. Воно вимагає застосування нових апаратних рішень засобів контролю, нагляду та збору даних. Для використання нових засобів захисту інформації при проектуванні комплексних систем захисту інформації. Головна увага приділяється методам контролю за потоками інформації, котрі досяжні атакам кіберзлочинців у сучасному кіберпросторі. Система контролю має функціональні властивості, що дозволяють здійснювати захист від кібератак при їх використанні у якості засобів захисту в рамках проектів на створення комплексних систем захисту інформації (КСЗІ).

Метою доповіді є викладення підходу щодо можливості створення системи контролю за інформаційними потоками з зазначеними властивостями.

Щодо реалізації зручно розглянути шлюз мережного комплексу МК LI-J призначений для забезпечення законного перехоплення («Lawful Intercept») телекомунікацій з мережного обладнання маршрутизаторів Juniper T640, T1600, Mx80, Mx240, Mx480, Mx960. МК LI-J розроблений у відповідності до ЗТВ «Технічні засоби для здійснення уповноваженими органами оперативно-розшукових заходів у телекомунікаційних мережах загального користування України. Загальні технічні вимоги» затверджені спільним Наказом Служби безпеки України та Міністерством транспорту та зв'язку України № 645/962 від 31 липня 2008 року. та стандартів ETSI (Європейського Інституту Стандартизації Електрозв'язку).

Перехоплення інформації в ІТС здійснюється за допомогою підключення до вузла мережного обладнання через порт. Відбір інформації в сеансах зв'язку за встановленими критеріями, комбінаціями ознак і фільтрами пошуку здійснюється в мережному обладнанні. Інформаційні потоки трафіку відібраних даних поступають на Шлюз мережного комплексу МК LI-J для подальшої обробки та передачі вмісту відібраних об'єктів перехоплення в систему управління системою перехоплення телекомунікацій (СУСП). Паралельно з передачею вмісту відібраних даних в СУСП від МК LI-J потрапляє службова інформація про відібрані сеанси зв'язку.

Основні функції:

- організація інтерфейсу взаємодії з серією маршрутизаторів компанії Juniper;

- формування по командах від СУСП ознак перехоплення в мережному обладнанні Juniper;

- взаємодію із системами Авторизації, Автентифікації та Акаунтінгу;

- прийом та обробка повідомлень протоколу Radius;

- прийом/передачу команд управління та контролю між засобами СУСП та мережним обладнанням;

- прийом та первинну обробку сеансів зв'язку від мережного обладнання;

- генерування супутньої інформації про відібрані сеанси зв'язку (IRI);

- захист від несанкціонованого доступу до програмних ресурсів системи та інформації, що зберігається в ній;

- дистанційний контроль та конфігурування всіх програмних модулів системи в реальному часі і доступ до відібраної інформації по кодових лініях зв'язку;

- автоматичне протоколювання дій користувачів та підсистем комплексу, за алгоритмами та формі, які є єдиними та уніфікованими з іншими комплексами, що застосовуються. Контроль справності каналів обміну інформацією між МК LI-J та СУСП. При відсутності зв'язку організовується збереження інформації до моменту відновлення.

Реалізація інтерфейсів функції LI (законного перехоплення) та їх взаємодія з обладнанням Juniper здійснюється при підключення МК LI-J до мережі. Таке підключення

МК LI-J здійснюється через порт підключенням до мережного інтерфейсу. Налаштування обладнання Juniper для взаємодії із МК LI-J відбувається одноразово адміністратором обладнання Juniper згідно наданої йому інструкції. Протокольна взаємодія МК LI-J по інтерфейсу X1(INI1) із обладнанням Juniper відбувається з використанням протоколу XML, механізмів JUNOScript, Python та Perl-скриптів.

Для передачі вмісту відібраного сеансу зв'язку по інтерфейсу X3(INI3) з обладнання Juniper до Шлюзу використовуються механізми інкапсуляції, а у випадку, коли використовується віддалене підключення обладнання Juniper до МК LI-J – також забезпечується механізми тунелювання та шифрування трафіку. Загальна схема взаємодії Шлюзу з обладнанням Juniper та іншим обладнанням оператора зв'язку (провайдера), власника мережі показана на Рис.1.

X1 – інтерфейс для передачі адміністративної інформації. Генерації супутньої інформації (IRI) здійснюється від двох інтерфейсів X2(INI2):

X2.1 – для отримання всього AAA-трафіку оператора зв'язку. Забезпечується відгалужувачем сигналу, встановленим на каналі зв'язку Juniper – Radius - Сервер;

X2.2 – для отримання всієї доступної інформації про клієнта оператора (об'єкта спостереження).

X3 – інтерфейс для передачі змісту сеансів зв'язку.

Шлюз мережного комплексу МК LI-J одночасно може забезпечувати роботу з декількома маршрутизаторами, в тому числі і різних моделей. Передача вмісту відібраних окремих об'єктів перехоплення на віддалені термінали суб'єктів перехоплення відбувається у відповідності до команд управління.

Таким чином, представлений шлюз мережного комплексу є загалом, найбільш адаптованим для вирішення таких задач.

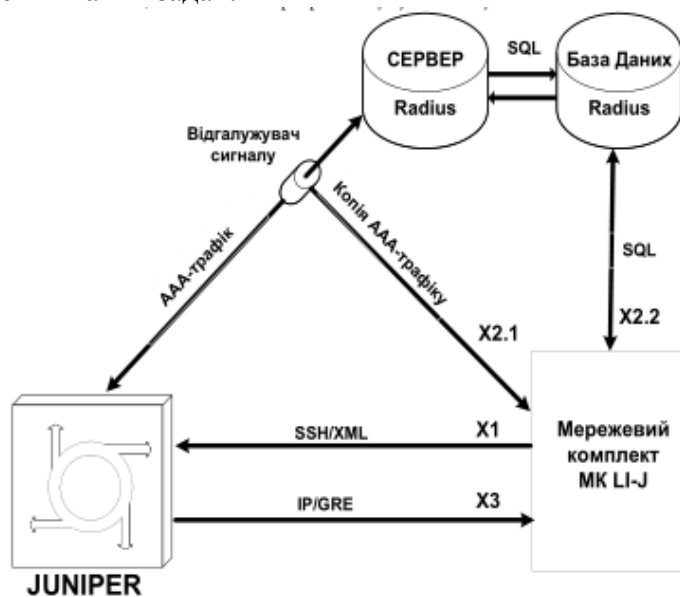


Рис. 1 Загальна схема взаємодії шлюзу мережного комплексу з обладнанням Juniper

Висновки: За такого підходу та при умові розробки відповідних ДСТУ і нормативно-методичної документації з'являється можливість вирішення задачі створення та впровадження системи нагляду за мережами КСЗІ на базі мереженого комплексу Juniper, а також нагляду за власною мережею Збройних сил України.

ЛІТЕРАТУРА

1. Луценко В.М., Балан А.В. Особливості системи контролю інформаційних потоків великого розміру. // „Захист інформації”, наук. практ. журнал., НАУ, Київ, Том 15, №3, (60), 2013, с. (231 – 235)

АЛГОРИТМ ПОБУДОВИ МАРШРУТУ РОЗВІДУВАЛЬНОГО РОБОТОТЕХНІЧНОГО КОМПЛЕКСУ В УМОВАХ НЕВИЗНАЧЕНОСТІ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Актуальність. Ведення бойових дій в міських умовах дуже складне і багатопланове завдання [1]. Як свідчать сучасні світові тенденції проведення військових операцій, виконання таких завдань є надзвичайно актуальними.

Заміна людини в бою роботом не тільки гуманна, вона цілком доцільна і забезпечує необхідну ефективність при виконанні завдань за призначенням.

Питання створення та використання робототехнічних комплексів (РТК) для ведення спеціальних і бойових дій проти супротивника на полі бою з наявністю лінії зіткнення сторін і також в урбанізованому військово-цивільному середовищі з хаотично змінюваною обстановкою, де відсутні звичні бойові порядки військ, наразі приймає пріоритетне значення [1].

Постановка завдання. Для вирішення задачі з проведення розвідувальної операції на місцевості з щільною забудовою запропоновано розглядати площину військових дій, як багатовимірний лабіринт. Пропонується вирішення завдання пошуку оптимального маршруту на прикладі виконання пошуку шляху в лабіринті з використанням елементів штучного інтелекту.

Нейронна мережа, будується з неформального опису алгоритму [2, 3, 4], та дозволяє виконувати пошук шляху в лабіринті. У теоретичних дослідженнях проходження лабіринту РТК використовує лабіринт, що для апроксимації математичних обґрунтувань розглядається як багатовимірний геометричний граф [4].

Основні положення. Пропонується варіант вирішення поставленого завдання за допомогою синтезу нейронної мережі [5, 6] на підставі попередньо синтезованого алгоритму.

Основна ідея, яка використовується при формуванні нейронної мережі, полягає в тому, що знайдений або досліджуваний шлях відзначається в нейронній мережі вагами одиниць, тупиковий - негативною вагою, а недосліджений - нульовими.

Кожна структура лабіринту розподіляється на зони. Важливою є точка збереження невизначеності. Саме при попаданні РТК в зону тупикового блоку відбувається повернення агента до точки невизначеності де виконується перезапуск процесу пошуку шляху, а тупиковий стан відзначається в лабіринті як недосяжний.

Основна ідея запропонованої нейронної мережі полягає в тому, що шлях від початкового стану до кінцевого формується в нейронній мережі за аналогією звичайного тесеракту в Евклідовому чотиривимірному просторі й визначається як опукла оболонка точок $(\pm 1, \pm 1, \pm 1, \pm 1)$.

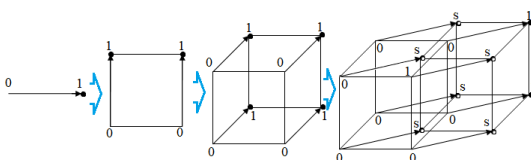
Тому вона може бути представлена у наступному вигляді:

$$[-1, 1]^4 \equiv \{(x_1, x_2, x_3, x_4) : -1 \leq x_i \leq 1\}.$$

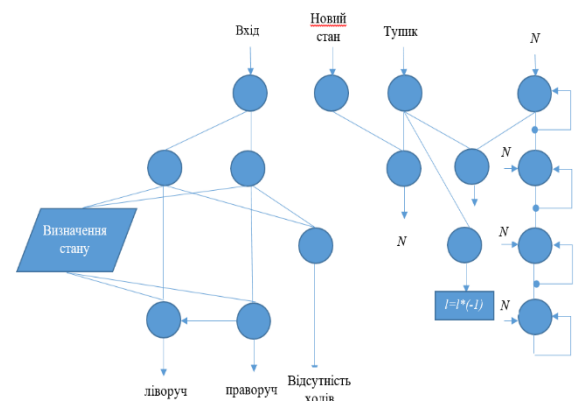
Глибина структури обмежена вісьмома нейро-структурними площинами $x_i = \pm 1, i = 1, 2, 3, 4$.

Декілька етапів процесу пошуку шляху в лабіринті, що ілюструють роботу синтезованої нейронної мережі зображено на рис.1.

У нейронній мережі початкове значення ваг шляхів мають значення „0”, але в процесі виконання



Кожна структура лабіринту розподіляється на зони. Важливою є точка збереження невизначеності. Саме при попаданні РТК в зону тупикового блоку відбувається повернення агента до точки невизначеності де виконується перезапуск процесу пошуку шляху, а тупиковий стан відзначається в



алгоритму, відображається як зміна ваг таким чином, шляхи, що ведуть до тупикових станів, задаються ваги зі значенням „-1”, а для шляхів, які досліджуються або ведуть до правильних станів, задаються ваги зі значенням „1”.

Так як області з однаковими вагами зв'язків кодують невелику кількість інформації, отже, мають невелике функціональне значення [5]. У той час області з величезними градієнтами значень ваги є надзвичайно інформаційними. Такі області можуть отримати вигоду від розміщення додаткових вузлів мережі для більш точного кодування природного процесу.

Довжина досліджуваного шляху визначається поточним активним нейроном (значення стану) в нижній частині нейронної мережі. При цьому перехід до наступного активного стану виконується якщо є ознака наявності нового стану і зникнення сигналу N , який свідчить про стан глухого кута.

Таким чином, рішення задачі в системі запропонованому алгоритмі може бути зведене до пошуку вирішального графа та вихідного пропозиційного графа [5, 7], оскільки, перегляд вирішального графа від кінцевих вершин до початкових точно задає безліч підзавдань, які необхідно вирішити для розв'язання вихідної задачі, і порядку їх вирішення. Необхідність пошуку вирішального графа визначається наявністю більше ніж однієї дочірньої вершини у діз'юнктивних вершин, або, іншими словами, наявністю альтернативних сукупностей підзавдань, вирішення яких необхідне для вирішення вихідної задачі.

Висновок. У статті запропоновано алгоритм вирішення завдання РТК з побудови оптимального маршруту в багатовимірному лабіринті в умовах невизначеності з використанням штучного інтелекту. Перетворення, що використані при синтезі нейронної мережі носить неформальний характер [4], а в результаті перетворення формується структура нейронної мережі, яка в подальшому може бути навчена традиційним способом або за допомогою розрахунку значень коефіцієнтів [6].

Запропонована структура нейронної мережі дозволяє вирішити задачу пошуку шляху виходу з лабіринту при постановці завдання, в якій на вхід нейронної мережі надходить тільки ознака успішного (або неуспішного) виконання минулої дії. Найпростіша ситуаційна модель поведінки агентів [7] є статичною і будується на основі "ситуація-дія". Такий алгоритм створює систему планування поведінки штучного інтелекту з доповненням механізму контролю ситуації. Запропонована формальна схема побудови математичних моделей процесів ситуаційного керування і планування дій інтелектуальних агентів.

При порівнянні найбільш популярних алгоритмів [3] навчання з підтвердженням можна зробити висновок про те, що запропонована мережа є рекурентною, що є новизною при вирішенні поставленого завдання. Також додатковою перевагою запропонованого підходу є те, що синтезовану нейронну мережу можна навчити за менше число ітерацій навчання [2], що може бути важливим для вирішення більш складних завдань і використання нейронних мереж більшого розміру.

ЛІТЕРАТУРА

1. The U.S. Army Robotic and Autonomous Systems Strategy, March 2017.
2. La Valle S. M. Planning Algorithms. Cambridge. U. K.: Cambridge University Press, 2006. 1007p.
3. Kleinberg J., Tardos E. Algorithm design Boston.: Cornell University, 2016
4. Claude Elwood Shannon Maze solving algorithm, 1975
5. Jennings N. R., Wooldridge M. J. Agent Technology, Berlin; Heidelberg; New-York: Springer-Verlag, 1998.
6. Muller J. P. The Design of Intelligent Agents: A Layered Approach, Springer-Verlag, Berlin, 1996
7. Alonso-Mora J. Collaborative Motion Planning for Multi-Agent Systems, Dr. Diss. Eidgenossische Technische Hochschule ETH Zurich. No 21705. 2014. 176 p.

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

ПЛАНУВАННЯ МІСЦЬ РОЗГОРТАННЯ ПІДРОЗДІЛІВ РАДІОРЕТРАНСЛЯТОРІВ НА ЛЬОТНО-ПІДЙОМНИХ ЗАСОБАХ

Нові принципи, які закладаються в основу управління військами (силами), вимагають суттєвого підвищення стійкості, розвідувальної захищеності і мобільності елементів системи зв'язку, а також її конфігураційної здатності. Основу перспективної польовий системи зв'язку повинна становити ешелонована, ієрархічно розподілена і рівнодоступна транспортна телекомунікаційна мережа, що є мережею загального користування угруповання військ (сил) в зоні відповідальності. Інфраструктурний принцип побудови системи зв'язку угруповання військ передбачає розгортання інформаційно-телекомунікаційної системи (ІТС) угруповання військ як багаторівневої ешелонованої (в космосі, в повітрі, на морі і землі) структури з метою формування єдиного інформаційного простору.

Повітряний ешелон ІТС базується на засобах повітряно-наземної зв'язку, технічному ресурсі ретрансляторів зв'язку та льотно-підйомних засобах (ЛПС).

Він використовується для обміну інформацією між різними мережами оперативної і тактичної ланок управління.

Ретранслятори можуть розміщуватися на літальних апаратах (повітряні пункти управління, БПЛА, аеростати), які експлуатуються спеціально створеними підрозділами, що входять в комплект військ зв'язку.

Планування бойового застосування повітряного ешелону системи зв'язку здійснюється органами управління зв'язком виходячи із завдань управління в майбутньої операції (бою).

Планування застосування повітряного ешелону ІТС є складовою частиною процесу планування зв'язку та інформаційних систем і являє собою процес функціонування органів управління зв'язком (начальника зв'язку), спрямований на формування обґрунтованих завдань підрозділам зв'язку БПЛА з організації зв'язку в об'єднанні, з'єднанні та частині.

На етапі визначення місць розгортання підрозділів радіо ретрансляторів на БПЛА посадковими особами органу управління зв'язком визначаються місця розгортання елементів ІТС загального користування.

При цьому в плані зв'язку вказуються всі елементи системи зв'язку в майбутній операції (бою), відповідні дані (склад елементів системи зв'язку, тип і характеристики апаратури зв'язку, робочі хвилі (частоти) і ін.) й розраховуються зони доступу, які наносяться на карти місцевості.

Проводиться оцінка місцевості, з якої немає доступу до ресурсу системи зв'язку. При здійсненні цієї оцінки використовуються заздалегідь розроблені методики визначення допустимих місць розгортання елементів системи зв'язку.

Формуються допоміжні матриці, що відображають інформацію про зони доступу кожного елемента ІТС.

В першу чергу визначається можливість розгортання підрозділів радіо ретрансляторів на БПЛА спільно з будь-яким елементами ІТС, що знаходяться в безпосередній близькості до визначеного району місцевості. При наявності декількох елементів ІТС, не об'єднаних в єдину систему, проводиться оцінка можливих зон доступу, які забезпечуються засобами підрозділів БПЛА. Послідовність дій при визначенні місць розгортання підрозділів радіо ретрансляторів на БПЛА представлена на рисунку 1.

При результатах, які не задовольняють висунутим вимогам за вихідними даними, визначаються допустимі місця розгортання підрозділів радіо ретрансляторів на БПЛА всередині визначених районів місцевості.

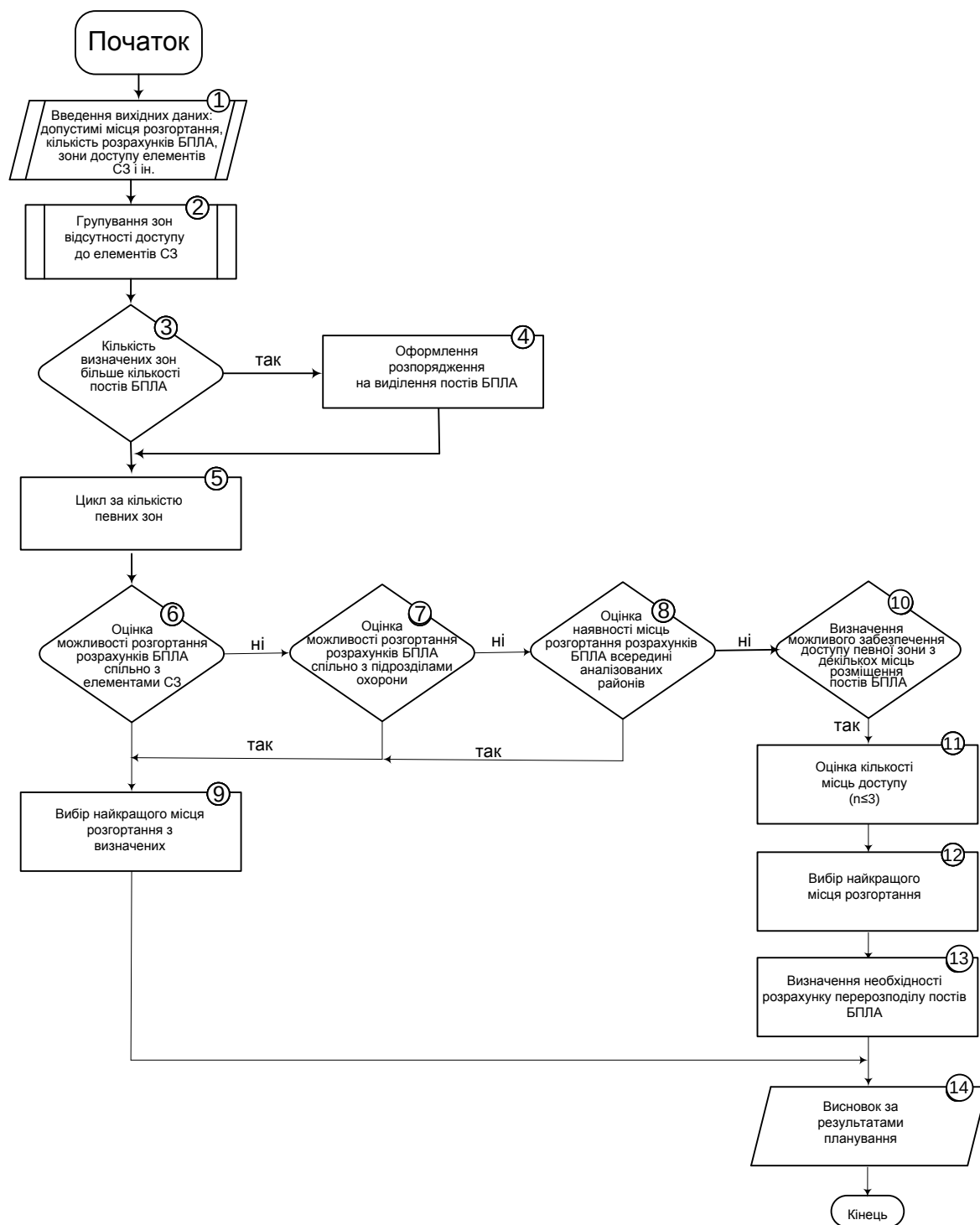


Рис.1. Блок-схема алгоритму визначення місць розгортання радіотрансляторів на БПЛА

При наявності декількох придатних місць розгортання підрозділів радіотрансляторів на БПЛА послідовно проводиться їх оцінка за ступенем забезпечення зон доступу, забезпечення якості ретрансляції радіосигналів, максимального часу баражування в районі застосування та ін. Таким чином проводиться оцінка кожного району місцевості, яка не має доступу до ресурсу ІТС і розподіл підрозділів радіотрансляторів на БПЛА.

НАПРЯМКИ ВДОСКОНАЛЕННЯ ТЕХНОЛОГІЙ САМОАДАПТАЦІЇ У МЕРЕЖАХ КХ РАДІОЗВ'ЯЗКУ

Моніторингові дослідження, що були проведені в 1996 року в рамках 9-ї Дослідницької комісії з радіозв'язку Міжнародного союзу електрозв'язку (МСЕ) показали, що в 41 % з контрольованих передач в КХ діапазоні хвиль трафік не передавався, а велася передача тільки неінформаційних сигналів або позивних. З огляду на крайню обмеженість радіоспектра КХ діапазону і велику потребу в його використанні актуальними стали питання застосування нових технологій спільного використання спектра без зниження показників якості радіоліній. Дослідження, що проводяться в США та інших державах привели до створення стандартів для автоматичних адаптивних систем КХ радіозв'язку (ALE радіосистем) у вигляді документів FED-STD-1045A, MIL-STD-188-141 A, MIL-STD-188-141B, MIL-STD-188_141C, STANAG 4538, які прийняті МСЕ базовими і котрі удосконалюються по теперішній час.

Адаптивними КХ радіосистемами є системи в яких автоматизовано процес пов'язаний зі зміною робочих параметрів і/або конфігурації у відповідь на динамічні зміни умов поширення сигналу в каналі і зовнішніх перешкод. Крім того, адаптивні системи здатні вести регулярний моніторинг завантаженості спектра і вибирати робочі частоти таким чином, щоб не створювати перешкод іншим користувачам.

Проект Концепції розвитку адаптивних КХ радіосистем НАТО „HF House” реалізується на основі функціонування еталонної моделі взаємодії відкритих систем OSI (Open Systems Interconnection). Взаємозв'язок и функціональні аспекти сучасної КХ технології в термінах еталонної семирівневої моделі наведено на рисунку 1.

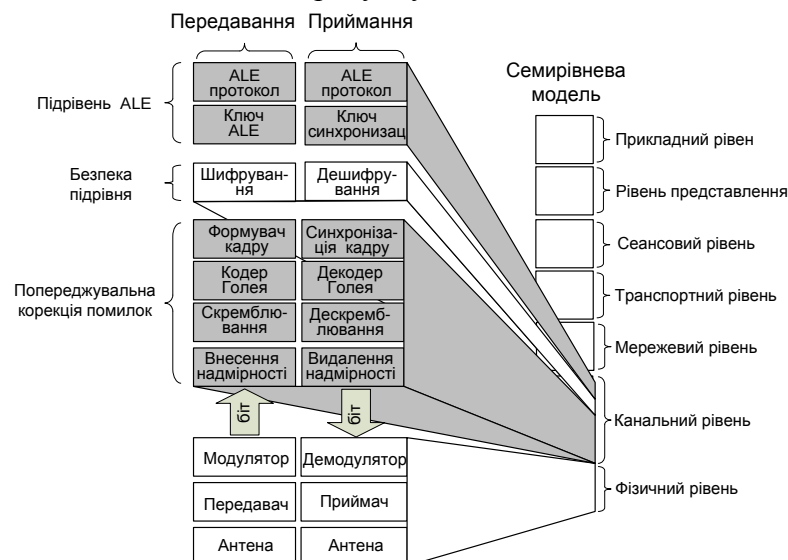


Рис.1 Функціональні аспекти і взаємодія елементів адаптивних КХ радіосистем на базі моделі OSI

Адаптивні методи, відповідні рівні і їх функції в КХ радіосистемах стандартизовані на фізичному, каналному, мережевому і системному рівнях з застосуванням технологій 2G HF і 3G HF. У таблиці 1 показані адаптивні методи і зв'язок відповідних рівнів і функцій.

Адаптивні методи, відповідні рівні і їх функції

Рівень	Адаптивний метод	Функція
Системний рівень адаптивності	Регулювання та управління частотами на системному рівні	Управління системою вищого рівня
		Регулювання частоти на системному рівні
		Оцінка впливу середовища
		Оцінка якості системи
Мережевий рівень адаптивності	Адаптивна маршрутизація	Схеми маршрутизації для передачі повідомлень
		Адаптивна маршрутизація
	Управління потоками	Управління потоками
	Установка з'єднання	Оцінка якості мережі
		Управління протоколами
	Обмін даними	Переконфігурація мережі
Канальний рівень адаптивності	Регулювання та управління частотами	Обмін даними
		Процедури управління частотами
		Іоносферне зондування
		Зондування каналу
		Оцінка якості каналу
Рівень адаптивності передачі	Регулювання та управління частотами	Контроль зайнятості / завантаження
		Швидкість передачі
		Форма сигналу
		Адаптивна зміна форми сигналу
		Завадостійке кодування
		Адаптивні схеми кодування
		Потужність
		Адаптивна регулювання потужності
		Тип антени
		Адаптивна регулювання діаграм спрямованості антени
	Оцінка якості передачі	Вимір енергетичного рівня каналу

Характерними загальносистемними властивостями адаптивних КХ радіосистем є:

підвищена живучість. За рахунок використання адаптивного вибору частоти, автоматичного повторення передачі за запитом (ARQ) і адаптивного вибору найбільш підходящих сигналів модуляції забезпечується підвищення готовності каналу зв'язку до передачі інформації;

гнучкість. Використання малопотужних станцій, як в стаціонарній, так і в мобільній компонентах системи зв'язку, за рахунок проведення безперервного аналізу та оновлення інформації про якість каналу зв'язку з метою вибору найбільш прийнятних частот для передачі трафіку;

менш високий рівень підготовки оператора. Адаптивні системи виконують функції встановлення, утримання і розривання каналу зв'язку без технічного втручання оператора.

Підвищення ефективності роботи існуючих систем КХ з застосуванням технологій 3G HF має досягатися за рахунок вдосконалення:

методів автоматичного вибору каналу (ACS) та автоматизації встановлення з'єднання (ALE); оптимізації випромінювань в результаті використання складних сигнально-кодових конструкцій; протидії ефектам багатопробного поширення радіохвиль, методом адаптивного вирівнювання посилення в смузі пропускання приймальних пристроїв.

Природно, що в рамках даних напрямків досліджень виникає задача визначення раціонального шляху, що забезпечує отримання необхідних характеристик адаптивних ліній КХ радіозв'язку стосовно до умов їх застосування зокрема та вимог до системи КХ радіозв'язку в цілому.

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ РЕЗЕРВУВАННЯ ІНФОРМАЦІЇ В СИСТЕМАХ РОЗПОДІЛЕНОГО ЗБЕРІГАННЯ ДАНИХ

Однією з основних умов ефективного функціонування розподілених комп'ютерних систем є забезпечення необхідного рівня збереження їх функціональних і інформаційних ресурсів. Різке збільшення об'ємів оброблюваних даних і необхідність їх сумісного використання великим числом споживачів приводять до необхідності вводити до складу комп'ютерних систем підсистеми розподіленого зберігання даних, які найчастіше будуються на устаткуванні мереж зберігання даних (МСД) (англ. SAN – Storage Area Network). Застосування методів розподіленого зберігання даних породжує ряд нових завдань забезпечення безпеки інформації, але одночасно і розширює можливості створення нових засобів і механізмів захисту. Зокрема, засоби розподіленого зберігання даних можуть бути ефективно застосовані для підвищення показників доступності і цілісності інформаційних ресурсів комп'ютерних систем різного призначення: інформаційних, управлінських, обчислювальних і контрольовано-вимірювальних.

Класичні підходи до забезпечення високого збереження інформаційних масивів засновані на методах ідентичної або неідентичної надмірності, відповідно до яких, як правило, для конкретної системи вибирається ефективна стратегія резервування. Безумовною гідністю більшості класичних методів резервування є їх простота, недоліками – високий ступінь дублювання інформації, неефективне використання ємкості магнітних носіїв, у ряді випадків – незадовільний великий час відновлення системи.

Системи розподіленого зберігання даних відкривають можливості для широкого використання методів відновного резервування, які поєднують надмірність з введенням аналітичних залежностей між блоками даних, що представляють інформацію, яка зберігається. Пропонується трирівнева модель забезпечення безпеки резервування, яка опирається на технічні можливості сучасних МСД. Оскільки пропонується підхід орієнтований на широкий клас розподілених систем, то в загальному випадку найважливішою вимогою до системи буде максимізація коефіцієнта готовності; далі за умови забезпечення заданого рівня доступності – вимога гарантій якості інформації, зокрема цілісності, і лише при виконанні цієї умови – реалізація певної політики управління доступом, включаючи забезпечення таємності.

Таким чином, мінімальною вимогою до системи є забезпечення заданого рівня доступності функціональних і інформаційних ресурсів. Підсистема забезпечення доступності ресурсів утворює перший рівень моделі. Необхідними умовами його реалізації є введення в систему:

- 1) засобів контролю і діагностики стану ресурсів системи;
- 2) оперативних резервів і засобів відновлення системи;
- 3) механізмів оцінки досягнутих параметрів доступності, які мають зворотний зв'язок з механізмами відновлення. Пропонується інтерполяційний метод безпечного розміщення інформаційних масивів в МСД, який складається з k пристроїв зберігання.

Також розроблені узагальнені алгоритми прямого і зворотного перетворень, які реалізують запропонований метод. Головними особливостями запропонованих алгоритмів є:

- представлення n -бітових блоків масиву у вигляді елементів кінцевого поля $GF(2^n)$, використання операцій в полі $GF(2^n)$ для перетворення блоків масиву;
- застосування процедури обчислення до „пробних точок” полінома над полем $GF(2^n)$ для отримання представлень блоків даних, які підлягають розміщенню на засобах зберігання (перетворення A);
- використання схеми Руффіні – Горнера множення багаточленів над полем $GF(2^n)$;

– побудова інтерполяційного полінома по Лагранжу $GF(2^n)[X]$ та обчислення коефіцієнтів полінома для отримання представлень блоків даних, які складають початковий масив (перетворення A^{-1});

– ідентифікація засобів зберігання, на яких розміщуються перетворені блоки даних, елементами кода Грея порядку n з метою скорочення обчислювальної складності перетворень A і A^{-1} .

Інтерполяційні методи розміщення даних вимагають реалізації методів контролю якості інформації на всіх етапах перетворення і відновлення інформації. Поняття якості інформації – багатоаспектне, зазвичай його прийнято характеризувати термінами „достовірність”, „збереження”, „логічна несуперечність”, „цілісність”, „актуальність” і іншими, набір яких сильно залежить від наочної області. Часто ці показники формулюються замовником інтуїтивно або керуючись дуже загальними поняттями міжнародних стандартів ISO 9000, ISO 9001, ISO 17799 і не визначаються кількісно. Очевидною умовою досягнення більшості вимог є забезпечення цілісності даних. Рішення цієї задачі ретельно відпрацьоване на елементарному рівні, але в МСД з’являється складне завдання синтезу схеми контролю достовірності на базі елементарних методів (циклічні надмірні коди, криптографічні хеш-функції і ін.), яка додатково повинна задовольняти вельми жорстким вимогам ефективності. Підсистема забезпечення якості інформації формує другий рівень моделі. Необхідними компонентами підсистеми є:

1) механізми контролю системних умов, які забезпечують можливість досягнення заданого рівня якості;

2) виконавчі механізми (наприклад, схема забезпечення цілісності);

3) механізми підсумкової оцінки якості інформації, які мають зворотний зв’язок з регулюючими і старанними механізмами.

В окремих випадках до проектованої системи висуваються вимоги по захисту від несанкціонованих дій (НСД) по відношенню до інформації і забезпеченню секретності (конфіденційності) інформації. Ідеальною умовою функціонування системи є постійна можливість доступу будь-якого користувача до будь-якого ресурсу системи (зрозуміло, якщо доступ не заборонений по вимогам безпеки інформації). Тому разом із забезпеченням високої доступності необхідне і вирішення до деякої міри „зворотного” завдання – обмеження і запобігання небажаному доступу до інформаційних ресурсів. В цьому випадку додатково потрібна підсистема управління доступом, здатна реалізувати специфіковану власником системи (власником ресурсів) політику управління доступом.

Управління доступом в складному розподіленому середовищі, прикладом якого є системи розподіленого зберігання даних, вимагає деякої адекватної формалізованої моделі. Класичні суб’єктно-об’єктні моделі з багатьох причин виявляються незручні для завдання і опису правил доступу в цих умовах. Застосування яких-небудь моделей або їх комбінацій для кожної конкретної системи завжди залежить від наочної області і відповідних нею цілей забезпечення безпеки. Таким чином, пропонується підхід може послужити основою розробки принципово нових методів забезпечення стійкості засобів захисту інформації в розподілених комп’ютерних системах при підвищених системних вимогах до функціональної і інформаційної безпеки.

ЛІТЕРАТУРА

1. Кульба В.В., Ковальовський С.С., Шелков А.Б. Достовірність і збереження інформації в АСУ. 2-е видавництво Серія „Інформаційні технології”. – М.: СИНТЕГ, 2003. – 500 с.

2. Запечников С.В. Исследование и разработка алгоритмов обеспечения безопасности доступа к информации в сетях хранения данных. – М.: МИФИ, 2003. – 195 с.

3. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: учебное пособие для вузов. – М: Горячая линия –Телеком, 2004. – 280 с.

МЕТОДИКА ОРГАНІЗАЦІЇ БЕЗПЕКИ МЕРЕЖ ЗВ'ЯЗКУ ПУНКТІВ УПРАВЛІННЯ НА ОСНОВІ ПРОГРАМНО-АПАРАТНИХ КОМПЛЕКСІВ

Мережа *Internet* створювалася як відкрита система, призначена для вільного обміну інформацією.

У силу відкритості своєї ідеології *Internet* надає для зловмисників значно більші можливості в порівнянні з традиційними інформаційними системами.

За цим питання про проблему захисту мереж і її компонентів постає досить важливим та актуальним в цей час, в час прогресу і комп'ютерних технологій.

Багато країн нарешті зрозуміли важливість цієї проблеми.

Відбувається збільшення витрат і зусиль спрямованих на виробництво і поліпшення різних засобів захисту.

Для досягнення мети в роботі сформульовані та вирішені часткові взаємопов'язані завдання дослідження:

- провести аналіз можливостей сучасних міжмережових екранів;
- розглянути характеристики міжмережових екранів;
- провести оцінку апаратури *Cisco ASA* для подальшого використання в зоні проведення ООС;
- розглянути варіанти налаштування *ME Cisco ASA 5505*.

Міжмережовий екран (МЕ) називають локальний або функціонально розподілений програмний (програмно-апаратний) засіб (комплект), який реалізує контроль за інформацією, що надходить в автоматизовану систему або виходить з автоматизованої системи.

Міжмережові екрани наступного покоління *Cisco ASA* – це чудово зарекомендовані у всьому світі динамічні міжмережові екрани з повним набором інтегрованих на високому рівні сервісів міжмережевого екранування наступного покоління для любого розміру мережі на одному чи декількох об'єктах.

Маючи адаптивну архітектуру, компанії можуть розгортати нові сервіси безпеки там, де це потрібно.

Наприклад, вони можуть добавляти різні сервіси запобігання сторжень та захисту від угроз, запропоновані в модулях *IPS*, за допомогою *AIP SSM* та *AIP SSC*, чи комплексні сервіси захисту від негативного ПЗ та забезпечення безпеки контенту, пропонувані в *CSC SSM*. Крім того, архітектура *Cisco ASA* пропонує нові сервіси по запобіганню нових загроз, надаючи компаніям виключні можливості захисту.

Таким чином, використання міжмережових екранів *Cisco ASA* забезпечать:

- дуже високі показники ефективності в захисті локальної мережі від зовнішніх атак;
- забезпечення до 150 Мбіт/с транзитного трафіку;
- робота на швидкості до 100 Мбіт/с при організації *VPN* доступу;
- орієнтованість на забезпечення мережевої безпеки користувачів;
- *NAT* трансляцію для об'єднаного доступу користувачів до мережі Інтернет;
- наявність вбудованого 8-ми портового коммутатора, при цьому 2 порти мають підтримку *PoE*, що забезпечує простоту підключення *IP* камери, *WI-FI* точки доступу чи *IP* телефону.

Він є досить простим у налаштуванні та експлуатації. Надає актуальні функції для користувача.

ПРОБЛЕМАТИКА РОЗВИТКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

Актуальність та постановка задачі.

Наразі активне проникнення інформатизації в усі сфери життєво важливих інтересів особистості, суспільства і держави привело до того, що в даний час усе більш актуального характеру набуває завдання забезпечення інформаційної безпеки України як невід'ємного елементу національної безпеки, а захист інформації перетворюється в одне із пріоритетних державних завдань.

Інформаційна безпека відіграє одну з ключових ролей у забезпеченні життєво важливих інтересів країни.

Це в першу чергу обумовлено швидким розвитком сучасних інформаційно-телекомунікаційних технологій, засобів зв'язку й інформатизації і, як наслідок, - істотним зростанням впливу інформаційної сфери на життя нашого суспільства.

В теперішній час інформація стає стратегічним національним ресурсом - одним з основних багатств економічно розвинутої держави, головним джерелом економічної і військової могутності держави.

Національний інформаційний ресурс повинен стати одним із вирішальних ресурсів розвитку країни, привабливою сферою вкладення капіталів суб'єктів господарської діяльності.

Тому метою подальших досліджень є процес забезпечення безпеки інформаційних ресурсів держави не тільки в правовій сфері, а й інформаційно-телекомунікаційній сфері в умовах інформаційних війн та інформаційного протиборства.

Основні положення.

Інформаційні війни відносяться до числа нових категорій конфліктного спектра, що розмиває кордони і предметні сфери традиційних понять економічного, військово-політичного і соціального конфліктів. У ХХІ столітті інформація стає однією з головних цілей і ключовим засобом ведення бойових дій.

Інформаційна війна стала результатом нових підходів до застосування інформації, визначена її роль і місце в суспільстві.

Нові тенденції в методах ведення сучасних інформаційних воєн, викликані розвитком інформаційних технологій, настільки масштабні, що дозволяють аналітикам говорити про нову гілку розвитку інформаційної безпеки.

Сутність цієї гілки полягає у появі нових технологічних рішень вже існуючих завдань у забезпеченні національної безпеки, в новому концептуальному розумінні цілей і задач оборонної політики.

Потенційними загрозами безпеці держави в інформаційній сфері є посилення технологічної залежності від іноземних країн та витіснення з національного ринку засобів інформатизації й телекомунікації вітчизняного виробництва.

Використовуючи впливові політичні та бізнесові зв'язки, представники закордонних компаній впроваджують у державні установи телекомунікаційне і комп'ютерне обладнання іноземного виробництва, чим створюють умови для можливого віддаленого несанкціонованого доступу до інформації, що циркулює в інформаційно-телекомунікаційних системах та комп'ютерних мережах органів державної влади й місцевого самоврядування. Таким чином, створюються реальні передумови для технічного проникнення до державних інформаційних ресурсів.

Поняття інформаційної війни відкриває новий тип соціально політичного невійськового конфлікту, що характеризується застосуванням сторонами мережових форм організації і відповідних їй доктрин, стратегій і технологій інформаційної епохи.

Необхідно також пам'ятати, що система інформаційної безпеки держави є складовою частиною загальної системи національної безпеки країни і мусить являти собою сукупність органів державної влади, які повинні узгоджено здійснювати діяльність по забезпеченню інформаційної безпеки на основі єдиних правових норм.

Дану систему необхідно розбудовувати на основі розмежування повноважень органів законодавчої, виконавчої і судової влади в області інформаційної безпеки, а також органів державної влади.

Для забезпечення безпеки національних інтересів в інформаційній сфері особливо важливою стає активізація діяльності суб'єктів в області інформаційної безпеки.

Виявлення й аналіз загроз інформаційної безпеки Україні, вироблення і вживання заходів, необхідних для адекватної відповіді на них, повинні розглядатися як найважливіші пріоритети національної безпеки.

Ефективно протистояти інформаційним загрозам у сучасних умовах може лише добре організована державна система забезпечення інформаційної безпеки, що повинна здійснюватися при повній взаємодії всіх державних органів, недержавних структур і громадян.

У сьогоднішніх умовах для забезпечення безпеки національних інтересів в інформаційній сфері особливо важливою стає активізація діяльності суб'єктів в області інформаційної безпеки.

Насамперед це стосується діяльності з питань захисту конституційних прав і свобод громадян, розвитку регіональних інформаційно-телекомунікаційних систем і забезпечення їх безпечного функціонування, формування регіональних відкритих інформаційних ресурсів і їх ефективного використання.

Проблема забезпечення інформаційної безпеки України багато в чому обумовлена пробілами в правовому регулюванні взаємодії органів виконавчої влади при вирішенні завдань забезпечення інформаційної безпеки.

Для вирішення цієї проблеми вважається доцільним здійснити такі заходи:

- створити ефективну багаторівневу державну систему забезпечення інформаційної безпеки, у якій будуть діяти єдині правові норми і механізми захисту інформаційних ресурсів, інформаційно-телекомунікаційної інфраструктури й інформаційних прав громадян, здійснюватися ефективна координація діяльності органів державної влади й управління.

- розробити механізм узгодження діяльності органів державної і місцевої влади в області забезпечення інформаційної безпеки;

- активізувати діяльність по формуванню державної політики в області забезпечення інформаційної безпеки регіонів, створенню необхідних для реалізації цієї політики організаційних структур і нормативної правової бази;

- зміцнювати взаємодію регіональних структур з державними органами виконавчої влади при вирішенні питань забезпечення інформаційної безпеки.

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ УПРАВЛІННЯ ЕЛЕМЕНТАМИ ВІРТУАЛЬНОЇ МЕРЕЖІ НА БАЗІ ПРОТОКОЛУ OPENFLOW

Актуальність теми: Мережеві технології дають можливість зробити значний крок вперед. Технології SDN дозволяють зменшити завантаженість мережі, та пришвидшити роботу мережі, завдяки принципу управління мережею на базі протоколу OpenFlow. Сучасний етап розвитку комп'ютерних систем можна охарактеризувати зростанням ролі розподілених мережевих структур унаслідок об'єктивного зниження темпів зростання продуктивності окремих вузлів та необхідністю організації їх спільної роботи для досягнення потрібних характеристик.

Мета: Створення віртуальної мережевої моделі SDN мережі та розробка програмно-апаратного модуля призначеного для організації управління на базі протоколу OpenFlow.

Виходячи з мети роботи, виникають **наступні завдання:** Аналіз архітектури SDN мережі; Аналіз принципу функціонування основних елементів мережі; Створення моделі SDN мережі, на базі протоколу OpenFlow; Конфігурування сегменту SDN мережі; Конфігурування контролеру SDN мережі.

Виклад основного матеріалу. Організація потоків даних в таких структурах вимагає нових підходів до управління із-за лавиноподібного збільшення комутаційних правил та трудомісткості управління мережевою інфраструктурою. Це пов'язано, з одного боку, з існуванням великої кількості різноманітних комунікаційних технологій, часто закритих та несумісних, з іншого боку – існуючі мережеве обладнання, як правило, спеціалізовані для „типових” локальних мереж і не дозволяють реалізувати багатокритеріальне та „багаторівневе” управління в складних гетерогенних структурах. Традиційний підхід до вирішення проблеми мережевих взаємодій припускає послідовну обробку одиниць передачі, зокрема пакетів, на кожному рівні еталонної моделі мережевої взаємодії ISO/OSI: комутатори другого рівня покликані виконувати фільтрацію та пересилку кадрів між портами на основі MAC-адресів, влучний VLAN та влучний QoS, класичні маршрутизатори використовуються для об'єднання сегментів мережі на основі IP-адресів, шлюзи забезпечують трансляцію мережевих адресів та контроль інформаційних потоків. На кожному рівні використовуються свої правила обробки (комутаційні матриці, таблиці маршрутизації, списки доступу та ін.) і різні формати даних. Одним їх напрямів „модернізації” класичного підходу до організації мережевої архітектури є створення програмно-конфігурованих мереж – ПКМ (англ. Software Defined Networks - SDN), що використовують протокол OpenFlow. До основних переваг мереж SDN відносять централізоване управління в мультівендорному середовищі, зменшення складності мережі за рахунок автоматизації, вищу швидкість впровадження інновацій, збільшення надійності та безпеки мережі, забезпечення узгодженості політик управління доступом, інжинірингу трафіку, параметрів якості послуг, безпеки та ін., вузько спрямоване (“точкове”) управління мережею, поліпшення якості сприйняття послуг користувачами.

Висновки. В роботі пропонується детально розглянути процес інсталяції, конфігурування та розгортання сегменту мережі SDN на базі протоколу OpenFlow, під'єднання різних активних елементів сегменту мережі SDN, використання веб інтерфейсу контролеру VAN SDN. Пропонується створити віртуальний сегмент мережі SDN та провести конфігурування основних її елементів. Топологія мережі буде розгорнута в емуляторі Mininet за допомогою скрипта мови програмування Python, також буде розгорнутий та під'єднаний до HPE VAN SDN controller який взаємодіє із мережею на базі протоколу OpenFlow.

ПОДАВЛЕННЯ ШУМУ В МОВНИХ СИГНАЛАХ НА ОСНОВІ ВИКОРИСТАННЯ МЕТОДУ SSA

На сьогоднішній день у ряді важливих для практики випадків використовуються методи подавлення шуму (методи фільтрації мовних сигналів (speech signals) на фоні акустичних завад (акустичного шуму)). Такі методи використовуються з метою покращення розбірливості мови, в якості попередньої обробки перед розпізнаванням мовних команд (у тому числі для мовних командних систем) і т.д.

Застосування методів подавлення шуму не обмежується завданнями обробки мовних сигналів. Вони використовуються при обробці зображень, в системах з антенними решітками, при оцінюванні стану каналу зв'язку в системі з OFDM (Orthogonal Frequency-Division Multiplexing – мультиплексування з ортогональним частотним розділенням сигналів) та в приймальному пристрої такої систем, обробці сигналів енцефалографічних систем і т.д.

Прикладами областей застосування методів фільтрації мовних сигналів є подавлення шуму, що має місце в кабіні літака (вертольота), при обробці мовних сигналів, в ході управління повітряним рухом (авіадиспетчерами і т.д.) та аналізі авіаційних катастроф з використанням бортових реєстраторів, розпізнавання мовних команд та розпізнавання особи, що говорить.

Найбільш відомими методами подавлення шуму є метод спектрального віднімання (spectral subtraction), методи, основані на короточасному перетворенні Фур'є (short time Fourier transformation (STFT)), методи фільтрації (Калмана, Вінера), методи основані на розкладенні Карунена-Лоева, метод сингулярного спектрального аналізу (SSA–singular spectrum analysis), вейвлет перетворення, методи, основані на використанні апарату скритих марківських моделей та інші.

Недоліком методів, основаних на спектральному відніманні, є поява в відновленому мовному сигналі спотворень (так званих музикальних тонів). Від таких недоліків вільні інші методи. Особливої уваги в технічній літературі отримав метод SSA.

Мета даної роботи, яка полягає в покращенні подавлення шуму в мовних сигналах та підвищенні розбірливості мови, досягається за рахунок використання методу SSA, пов'язаного з методом головних компонент (перетворенням Карунена-Лоева). Його реалізація пов'язана з спектральним розкладенням матриці даних (singular value decomposition (SVD)). Особливістю використання методу SSA при обробці мовних сигналів, як і при оцінюванні стану каналу зв'язку, є більший розмір вікна у порівнянні з випадком, коли сигнал містить декілька гармонічних компонент. В пропонуємій модифікації методу SSA на етапі відновлення сигналу замість відкидання компонент, що відповідають підпростору шуму (truncated SVD), використовується зменшення сингулярних чисел підпростору шуму з використанням вагових коефіцієнтів.

Оцінка ефективності запропонованої модифікації методу SSA здійснена в ході моделювання в MathLab. Отримані результати моделювання вказують на те, що використання запропонованого підходу дозволяє покращити розбірливість мови, яка визначалась за допомогою індексу розбірливості мови (speech intelligibility index). Переваги використання запропонованої модифікації методу SSA також показано з використанням спектрограм оригінального та відновленого мовного сигналу.

До напрямків подальших досліджень слід віднести узагальнення запропонованого підходу на випадок кольорового шуму, сумісне використання методу SSA з іншими методами або компонентами даних методів, використання запропонованого підходу при вирішенні завдання розпізнавання мовних команд (сигналів). Крім того, викликає інтерес аналіз випадку використання декількох мікрофонів (решітки мікрофонів).

PROGRESSIVE WEB APPLICATIONS – ТЕХНОЛОГІЯ ДЛЯ СТВОРЕННЯ СУЧАСНИХ КЛІЄНТ-СЕРВЕРНИХ ДОДАТКІВ

Актуальність Розвиток інформаційного суспільства спонукає військову сферу використовувати сучасні інформаційні та телекомунікаційні технології під час професійної підготовки і подальшої службової діяльності. Особливий напрям займає розробка додатків на основі клієнт-серверної архітектури. У сучасному світі існує велика кількість технологій для розробки клієнт-серверних додатків. Традиційні уявлення у сфері інформаційних технологій починають кардинально змінюватись. Кожного року з'являються нові технології, які прискорюють функціонування та розробку додатків. Розробка веб-додатків за допомогою звичайних веб-технологій стає незручною, а швидкість роботи таких додатків повільною. У даний час актуальними є багатофункціональні додатки, але не зміну їм з'являються прогресивні додатки, які значно поліпшують користувацький інтерфейс доступу. Вони працюють однаково просто та зрозуміло у всіх середовищах функціонування. З Progressive Web Applications досить створити один додаток, який буде працювати на всіх визначених операційних системах. Progressive Web Applications поєднують в собі простоту використання веб-сайтів та технічні можливості native applications. Зовні Progressive Web Applications схожі на звичайні, але можуть працювати навіть без підключення до мережі, забезпечуючи роботу в offline-режимі, що є досить актуальним для більшості електронних пристроїв.

Мета дослідження полягає у вдосконаленні процесу висвітлення інформації на основі технології розробки Progressive Web Applications, виходячи з цього були поставлені **наступні часткові завдання**:

- аналіз існуючих технологій розробки додатків на основі клієнт-серверної архітектури;
- дослідження наявних рішень та підходів, що можуть спростити розробку кросплатформних додатків;
- автоматизація процесів реалізації функціональності Progressive Web Applications на клієнт-серверному додатку;
- розробка клієнт-серверного додатку на основі технології Progressive Web Applications.

Виклад основного матеріалу. Progressive Web Applications – це технологія, яка передбачає розробку програмного і веб додатку разом. Вона надає можливість на веб-додаткові реалізовувати функціонал звичайного додатку, який встановлюється на пристрій з будь-якою операційною системою.

Progressive Web Applications допомагають вирішити такі проблеми, як низька швидкість інтернету, довге завантаження сайту та інтерактивність, що є вагомою причиною для використання прогресивних веб-додатків.

Основними можливостями, що надають Progressive Web Applications є:

- швидкість – PWA завжди швидко завантажуються;
- надійність – завдяки технології Service Workers можливо повністю завантажити зображення на екрані користувача, навіть при відсутності доступу до мережі;
- інтеграція – з PWA контент додатку завантажується поступово.

Одним із важливих факторів є гарантія безпеки, особливо коли це стосується крадіжки особистих даних, їх розповсюдження та злом. PWA мають змогу протистояти цій проблемі.

Висновки. Отже, в рамках даної роботи запропоновано використання Progressive Web Applications, як основну технологію для створення клієнт-серверних додатків. Дана технологія робить процес доступу до функцій програми полегшеними для користувачів. Створені додатки надають доступ до контенту і сервісу, що полегшує їх використання.

ОРГАНІЗАЦІЯ СПЕЦІАЛІЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ДЛЯ ПІДТРИМКИ ДИСТАНЦІЙНОЇ ОСВІТИ

Актуальність. У більшості випадків, за будь-яких епідемій або масових захворювань першими установами, які закриваються, є школи, коледжі, ВНЗ тощо. Проблему організації дистанційного навчання перед більшістю освітніх установ в Україні надзвичайно актуальною зробила ситуація, що склалася в умовах загрози епідемії коронавірусу COVID-19. З метою запобігання епідемії в більшості регіонів країни вводиться дистанційне навчання. Варто зауважити, що у випадку прийняття рішення переходу на віддалене навчання, місцевій владі слід вибудувати роботу так, щоб це не позначилося на освітньому процесі, задіюючи онлайн-формати, відеокурси, а також різного роду месенджери. Адже ресурсів для здійснення дистанційного навчання в даний час достатньо.

Постановка задачі. Активне впровадження сучасних технічних засобів в систему освіти докорінно змінило підхід до освітнього процесу.

В умовах епідемії коронавірусу, щоденне вдосконалення цифрових технологій, в тому числі розвиток і вдосконалення дистанційної шкільної, вузівської, додаткової та інших видів освіти, є одним з найважливіших напрямків розвитку сучасного навчання в усьому світі.

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

Основні положення. Головна особливість дистанційного навчання – можливість отримання освітніх послуг без відвідування навчального закладу, оскільки вивчення предметів і спілкування з викладачами повністю здійснюється в мережі Інтернет. За допомогою дистанційного навчання вдається вирішувати такі педагогічні завдання, як формування пізнавальної самостійності і активності, створення ефективного освітнього простору, розвиток критичного мислення та здатності конструктивно відстоювати власну точку зору. До основних форм дистанційного навчання відносять відеолекції, відео конференції, чати і вебінари.

Актуальним вважається інноваційний підхід до викладання спеціалізованих дисциплін з використанням навчальних середовищ на основі віртуальної реальності, які можуть бути використані для покращення навчального досвіду учнів, студентів та курсантів. При всьому різноманітті існуючих підходів вважається, що STEM-освіта – це сучасний освітній феномен, завдяки якому підвищується якість розуміння слухачами дисциплін, зокрема точних.

Це дозволяє підготувати майбутніх фахівців до більш ефективного застосування отриманих знань при вирішенні професійних завдань і проблем, а також значно підвищити рівень навичок високоорганізованого мислення і розвиток компетенції в STEM.

Направленість навчального процесу на самостійну роботу і підвищення її ефективності передбачає збільшення числа годин на самопідготовку слухачів навчальних курсів. З метою теоретичної підтримки самостійної роботи впроваджено систему віртуального навчального середовища (ВНС) (virtual learning environment) – програмної системи, що створена для підтримки процесу дистанційного навчання.

Висновки. Прикладом впровадження віртуального навчального середовища в роботу навчального закладу можна розглядати роботу навчального середовища Moodle в Національному університеті „Львівська політехніка” (<http://vns.lpnu.ua/>), а також використання вказаних інформаційних технологій під час впровадження дистанційної освіти в Національній академії сухопутних військ імені гетьмана Петра Сагайдачного (<http://www.asv.gov.ua/>), Львівському коледжі транспортних інфраструктур (<https://www.lkti.lviv.ua/>) та інших навчальних закладах.

ВИКОРИСТАННЯ СКЛАДНИХ ОРТОГОНАЛЬНИХ СИГНАЛЬНО-КОДОВИХ КОНСТРУКЦІЙ ПРИ ПОБУДОВІ ЗАВАДОЗАХИЩЕНИХ КАНАЛІВ УПРАВЛІННЯ ТАКТИЧНИХ БПЛА

Актуальність, постановка задачі. Світова тенденція застосування безпілотних авіаційних та робототехнічних комплексів (дронів) з використанням елементів штучного інтелекту у збройних конфліктах надає все більшого поштовху до проведення досліджень в сфері безвідмовного дистанційного керування та контролю за параметрами зазначених комплексів, удосконаленню існуючих каналів управління та новітніх підходів при проектуванні та створенні зазначених каналів.

Як показує сучасний рівень розвитку безпілотних авіаційних комплексів (БпАК) та засобів боротьби з ними, одним з важливих завдань є забезпечення скритного та завадозахищеного керування тактичним безпілотним літальним апаратом (БпЛА) або групою БпЛА в умовах роботи засобів радіорозвідки та постановки навмисних завад противником.

Використання шумоподібних та завадозахищених сигналів з розширенням спектру при побудові каналів управління тактичними БпЛА, утворених модуляцією несучої частоти псевдовипадковою послідовністю, все частіше знаходять своє застосування з метою вирішення завдань дистанційного керування тактичними БпЛА.

Даний підхід, що використовує внутрішньоімпульсну лінійну частотну модуляцію (ВЛЧМ), знайшов своє широке застосування в бездротових сенсорних мережах військового призначення та є потенційно можливим при проектуванні та створенні завадозахищеного каналу управління тактичним БпЛА за рахунок своїх високих енергетичних показників. Високі енергетичні показники дозволяють реалізувати детектування приймачем наявності корисного сигналу в просторі з низьким відношенням потужності сигналу до потужності завади в широкій смузі частот, що відкриває можливість передавати команди управління тактичним БпЛА на значні відстані при низьких потужностях випромінювання передавачем в умовах роботи засобів радіорозвідки та постановки навмисних завад противником.

Канали управління, утворені з використанням ВЛЧМ сигналів, є актуальними лише для тактичних БпЛА з відстанями між БпЛА та наземною станцією керування (НСК) лише до декількох десятків кілометрів.

Основні характеристики, що забезпечують значні відстані для забезпечення зв'язку, досягаються за рахунок високих енергетичних показників ВЛЧМ сигналів, таких як спектральна щільність потужності та зосередження енергії на передачу одного біту інформації з заданою достовірністю (ймовірністю бітової помилки), що в свою чергу призводить до зниження швидкості передачі даних між НСК та БпЛА.

Мета. Метою роботи є вирішення завдання по забезпеченню достатньої швидкості передачі даних в каналі управління тактичним БпЛА, що є критично важливим з точки зору безвідмовного дистанційного керування та контролю параметрів тактичного БпЛА.

Основні положення. Аналіз світових досліджень показує високу зацікавленість науковців до класу ВЛЧМ сигналів при проектуванні каналів обміну інформацією між сенсорами різноманітного призначення. Роботи, в цілому, присвячені дослідженням продуктивності та якості надання послуг в мережах з тисячами кінцевих пристроїв з низькими показниками енергоспоживання та тривалим часом автономної роботи, сенсорів в різноманітних сценаріях їх застосування. Ряд авторів проводять дослідження впливу різноманітних параметрів ВЛЧМ сигналів та кількості одночасної роботи кінцевих пристроїв на дальність забезпечення зв'язку при мінімальних показниках випромінюваної потужності сигналу. Крім цього, пропонується ряд імітаційних моделей функціонування каналів управління БпЛА при досягненні максимального віддалення БпЛА від НСК. Але, слід зауважити, що в даних роботах не вирішуються завдання збільшення швидкості передачі

інформації між БпЛА та НСК в каналі управління, утвореному з використанням ВЛЧМ сигналів при значному віддаленні БпЛА від НСК за умов нестаціонарності каналу зв'язку та наявності навмисних завад.

Перш за все, при проведенні аналітичних розрахунків швидкості передачі даних в каналі управління тактичним БпЛА, слід звернутися до класичного підходу, запровадженому К. Шенноном. В своїх роботах він довів, що з метою досягнення потенційно можливої швидкості передачі даних сигнали повинні наближатися по своїх статистичних властивостях до білого шуму, де ймовірність бітової помилки буде нескінченно малою при нескінченно великій довжині послідовності, що передається. Крім цього, він стверджував, що існує граничний показник, що характеризує швидкість передачі інформації по каналу зв'язку, який залежить від величини випромінюваної потужності передавача, ширини полоси пропускання каналу зв'язку та інтенсивності адитивного шуму, названий потенційною пропускнуою спроможністю каналу зв'язку.

Крім цього, потенційна пропусчна спроможність каналу зв'язку залежить лише від ширини смуги пропускання каналу та потужності корисного сигналу на вході приймача та взагалі не залежить від частоти, на якій передається сигнал. Тому, враховуючи високі енергетичні показники ВЛЧМ сигналів та можливість детектування приймачем цих сигналів нижче рівня білого шуму, що обумовлені видом модуляції, враховуючи критерії та обмеження для каналу управління тактичним БпЛА, можна отримати потенційну пропускну спроможність каналу управління тактичним БпЛА, що становить близько 400 кбіт/с та цілком задовольняє вимогам до завадозахищених каналів управління тактичними БпЛА.

Звісно, що в реальних умовах швидкість передачі даних в каналі управління тактичним БпЛА буде значно меншою, тому пропонується створити аналітичну модель розрахунку швидкості передачі даних в каналі управління тактичним БпЛА з метою подальшого проведення імітаційного моделювання за допомогою програного забезпечення *MATLAB* та *Simulink*.

Враховуючи те, що ВЛЧМ сигнали відносяться до класу складних сигналів пропонується розглядати аналітичну модель на декількох рівнях, таких як рівень, що охоплює фізичні явища та особливості процесів розповсюдження ВЛЧМ сигналів в просторі та рівень формування інформаційного кадру з врахуванням особливостей дистанційного керування та отримання інформації від сенсорів та датчиків тактичного БпЛА. В свою чергу, дослідження спрямовано на отримання кількісної оцінки енергетичних показників ВЛЧМ сигналів та символічної швидкості передачі даних в каналі управління тактичним БпЛА.

Враховуючи вищевикладене, на рівні фізичних явищ розповсюдження сигналів в просторі з метою підвищення ймовірності детектування наявності корисного сигналу приймачем пропонується компонування існуючого методу дискретного перетворення Фур'є з впровадженням елементів вейвлет-перетворень. Вейвлет-перетворення являє собою особливий тип лінійних перетворень та може дати нам з частотою сигналів час (на відміну від дискретних перетворень Фур'є, що локалізовані за частотами та не локалізовані в часі), пов'язаний з цими частотами, що робить його дуже зручним для застосування при оцінці широкосмугових сигналів. Це, в свою чергу дозволить збільшити евклідову відстань між сигнальними точками та збільшити енергетичні параметри сигналу. Крім цього, на рівні формування інформаційного кадру пропонується застосувати коефіцієнт перекриття в часі внутрішніх імпульсів ЛЧМ сигналів, що дозволить підвищити символічну швидкість.

Висновки. Таким чином, реалізація запропонованих підходів дозволить збільшити швидкість передачі даних в завадозахищеному каналі управління тактичним БпЛА при заданих обмеженнях частотного ресурсу та випромінюваної потужності передавача. Напрямок подальших досліджень є створення імітаційної моделі розрахунку швидкості передачі даних з врахуванням наведених припущень за допомогою програмного забезпечення *MATLAB* та *Simulink* та обґрунтування її адекватності. В свою чергу, отримані результати буде покладено в основу формування методики підвищення швидкості передачі даних в завадозахищеному каналі управління тактичним БпЛА.

ІНТЕЛЕКТУАЛЬНА МЕРЕЖА МУЛЬТИФУНКЦІОНАЛЬНИХ СЕНСОРНИХ ВУЗЛІВ ДЛЯ СИСТЕМ МОНІТОРІНГУ ТА ПІДТРИМКИ РІШЕНЬ

Актуальність. Моніторинг параметрів нерухомих та рухомих об'єктів є важливою складовою у цивільних та військових системах контролю та управління. Для постійного моніторингу стану та ідентифікації об'єктів використовуються бездротові сенсорні мережі (WSN) з мультифункціональними сенсорними вузлами з автономним живленням, що забезпечують передавання даних через бездротову комунікаційну мережу. В системи входять також вузли для координації роботи мережі та обробки даних. Подібні системи можуть забезпечувати безперервний моніторинг об'єктів, що розподілені на великих територіях.

Мета роботи: Дослідження можливостей побудови системи з мережею бездротових сенсорів для ідентифікації та моніторингу об'єктів на основі контролю та аналізу акустичних, вібраційних та електромагнітних аномалій.

Основні положення. Система включає інтелектуальні сенсорні вузли, комунікаційні вузли, та вузли обробки даних. Сенсорні вузли з автономним живленням мають суттєві обмеження ресурсу джерела живлення, потужності процесора та швидкості передачі даних. Ці недоліки відсутні у центральних вузлів обробки даних.

В інтелектуальній мережі мультифункціональний сенсорний вузол забезпечує вимірювання параметрів, виділення аномалії, попередню обробку та аналіз даних, виділення відбитку аномалії, передавання відбитку аномалії через комунікаційну мережу на вузол обробки даних з потужним CPU, що виконує обробку відбитку та ідентифікацію характеристик об'єкту на основі попередньо сформованої бази даних, реєстрацію та візуалізацію параметрів об'єкту.

Сенсорні вузли можуть вимірювати різні параметри в залежності від призначення. Сенсорний вузол, що включає масив мікрофонів, модуль GPS, трьохосні MEMS магнітометри, акселерометри та гіроскопи, барометр та датчики температури і вологості може використовуватись для реєстрації звукових аномалій, а на їх основі визначення координат джерела звуку та ідентифікації його характеристик.

При визначенні орієнтації сенсорного вузла використовується алгоритм фільтру Маджвіка для IMU з магнітомерами, гіроскопами та акселерометрами (MARG) на основі кватерніонів. При обробці даних GPS використовується фільтр Калмана.

Для визначення координат об'єкта – джерела звуку, розроблений алгоритм, що розраховує орієнтацію та координати джерела звуку за різницею часу між звуковими хвилями, що вимірюються масивом мікрофонів.

Для ідентифікації параметрів об'єкта – джерела звуку, використовується алгоритм виділення відбитку аномалії на основі спектрального аналізу сигналів та пошуку відповідного відбитку в попередньо сформованій базі відбитків джерел звуку.

Вказаний сенсорний вузол може також використовуватись для аналізу та визначення аномалій вібрацій ґрунту та магнітного поля, що створюються рухомими об'єктами. В систему можуть бути інтегровані як mesh вузли, так і вузли з іншими типами прийомо-передавачів та відповідними шлюзами, наприклад LoRaWAN.

Для безпеки передачі даних на рівні бездротової мережі використовується шифрування даних 128/256 bit AES, на рівні TCP/IP - захист на транспортному рівні TLS.

Параметри об'єктів реєструються на сервері системи в базі даних SQL, для візуалізації даних використовується GUI на основі веб-сервера. Клієнти системи можуть отримувати дані про об'єкти на мобільні пристрої. Система може також забезпечувати обмін даними з іншими інформаційними системами.

Висновок. В роботі розглянуто архітектуру інтелектуальної мережі мультифункціональних сенсорних вузлів та наведено приклади сенсорних вузлів для визначення координат та ідентифікації параметрів об'єктів, їх реєстрації та візуалізації.

ПІДСИСТЕМА ОБМІНУ СТАНДАРТИЗОВАНИМИ ПОВІДОМЛЕННЯМИ

Актуальність дослідження обумовлена необхідністю підвищення ефективності обміну інформацією між підрозділами Збройних Сил України, а також створенням можливості для ефективної взаємодії між іншими підрозділами сектору безпеки та силами союзників. Можливість передавати накази та звіти у виді повідомлень між підрозділами та союзними силами є наріжним каменем усіх військових операцій. Оперативна сумісність між країнами, підрозділами та технікою є критично важливим фактором під час виконання військових місій. Важливо подавати інформацію у вигляді стандартизованих повідомлень, які допомагають отримувачам чітко розуміти зміст. Таким чином, удосконалення підсистеми обміну стандартизованими повідомленнями згідно стандарту NATO „*Message Catalogue (APP-11)*” для покращення взаємодії, як між підрозділами сектору оборони так і з підрозділами країн НАТО є актуальним науково-технічним завданням.

Мета дослідження полягає у підвищенні ефективності процесів створення стандартизованих повідомлень за рахунок виконання **наступних часткових завдань дослідження:**

- аналіз сучасного підходу до передачі наказів та звітів у підрозділах Збройних Сил України та НАТО;
- вдосконалення алгоритму створення користувацького інтерфейсу з урахуванням недоліків та обмежень моделей існуючої підсистеми;
- вдосконалення алгоритму обробки повідомлень з урахуванням недоліків та обмежень моделей існуючої підсистеми;
- автоматизація процесів трансформації повідомлень у інформаційно-телекомунікаційних системах військового призначення згідно до стандарту NATO „*Message Text Formatting System (ADatP-3)*”
- розробка архітектури та структури підсистеми обміну стандартизованими повідомленнями.

Виклад основного матеріалу. Сучасна воєнно-політична ситуація, що склалася навколо і в середині України безпосереднім чином впливає на розвиток ЗСУ у найближчі роки. Президентом України визначено напрямок реформування та розвитку збройних сил, а саме приведення ЗСУ у відповідність до стандартів НАТО з метою отримання членства у альянсі. Було досліджено документ MC 0640 „Мінімальний рівень спроможностей систем зв'язку та інформації наземних військ тактичної ланки”, в якому описано варіанти налагодження зв'язку між підрозділами. Серед описаних варіантів було обрано систему форматів текстових повідомлень (*MTFS, Message Text Formatting System*). *MTF* передбачає застосування єдиного набору форматів повідомлень, що надаються у вигляді *XSD* схем. *MTF ADatP-3* можуть бути представлені як текстові повідомлення з роздільником-косою рисою (вихідний формат) або як документи *XML*. Використовуючи класичний підхід до проектування складних систем було розроблено узагальнену архітектуру, структуру і алгоритм функціонування підсистеми обміну стандартизованими повідомленнями з розширеним функціоналом.

Висновки. Отже, у ході розширення функціоналу підсистеми обміну стандартизованими повідомленнями згідно до стандарту NATO „*Message Catalogue (APP-11)*” виконано дослідження вже існуючих підходів до вдосконалення процесів створення стандартизованих повідомлень. У якості основи для розробки було обґрунтовано використання системи форматів текстових повідомлень (*MTFS, Message Text Formatting System*), що надаються у вигляді *XSD* схем. Реалізовано підсистему обміну стандартизованими повідомленнями, з можливістю використання супутникового каналу передачі даних.

ПІДСИСТЕМА ОБЛІКУ ЗАСОБІВ КОМП'ЮТЕРНОЇ ТЕХНІКИ НАВЧАЛЬНО-ЛАБОРАТОРНОГО КОМПЛЕКСУ КАФЕДРИ ВВНЗ

Актуальність дослідження обумовлена необхідністю вдосконалення системи обліку матеріальних засобів у підрозділах Збройних Сил України і, як слідство у підвищенні ефективності задачі обліку та руху засобів комп'ютерної техніки НЛК кафедри ВВНЗ.

Витрати часу, кількості працівників, можливого допущення помилок та самої складності реалізації процесу під час процесу ручного обліку за допомогою паперових журналів (книг, форм) збільшується. Звідси випливає, що узгодження рішення задач автоматизації обліку комп'ютерної техніки навчально-лабораторного комплексу кафедри ВВНЗ є важливим питанням, що визначає ефективність підсистеми обліку матеріальних засобів у Збройних Силах України в цілому.

Мета дослідження полягає у вдосконаленні процесу обліку засобів комп'ютерної техніки навчально лабораторного комплексу кафедри ВВНЗ за рахунок виконання наступних **часткових завдань дослідження**:

- аналізу існуючого підходу до обліку матеріальних засобів у Збройних Силах України та аналізу керівних документів що регламентують даний процес;

- дослідження вже існуючого програмного забезпечення для ведення обліку комп'ютерної техніки та вказання їхніх недоліків;

- вдосконалення алгоритму обліку майна та процесів, що пов'язані з цією задачею, з урахуванням недоліків та обмежень існуючих моделей;

- автоматизація процесів обліку та руху матеріальних засобів у підрозділах ЗСУ, за рахунок розробки підсистеми обліку засобів комп'ютерної техніки навчально-лабораторного комплексу кафедри ВВНЗ;

Виклад основного матеріалу. Облік військового майна у Збройних Силах України є складовою частиною бухгалтерського обліку. Обліку підлягає все військове майно незалежно від його призначення та джерел надходження. Цей процес повинен бути своєчасним, достовірним і точним.

Облік матеріальних засобів у Збройних Силах України ведеться з метою своєчасного забезпечення відповідних посадових осіб та органів управління достовірними даними про наявність, рух та якісний (технічний) стан матеріальних засобів, які необхідні для планування і організації забезпечення ними військ; контролю за збереженням, законністю, достовірністю та ефективністю витрачання матеріальних засобів; підготовки вихідних даних для складання звітних документів, які встановлені табелем термінових донесень.

Застосування даної підсистеми повинно зменшити число помилок, пов'язаних з неякісним обліком засобів комп'ютерної техніки кафедри, а також збільшити продуктивність праці за рахунок автоматизації процесу ручного обліку за допомогою паперових журналів (книг, форм). В даній роботі для вирішення завдання автоматизації процесу ручного обліку запропоновано використання клієнт-серверного підходу. Базуючись на етапи проектування структури підсистеми, використовуючи класичний підхід проектування було розроблено узагальнену архітектуру і алгоритми роботи підсистеми обліку засобів комп'ютерної техніки НЛК кафедри ВВНЗ.

Висновки. Отже, у ході підготовки та викладення матеріалів доповіді виконано дослідження процесу обліку матеріальних засобів у ЗСУ та вже існуючих підходів. З'ясовано актуальність обраної теми доповіді та перспективи подальшого застосування викладених матеріалів. Після проведеного аналізу можливостей підсистеми та актуальності її застосування можна впевнено зробити висновки про великий потенціал у сучасному світі, зокрема у Збройних Силах України.

АНАЛІЗ МОЖЛИВОСТІ ВИКОРИСТАННЯ АЛГОРИТМУ SPHINCS+ В ІНФРАСТРУКТУРІ ВІДКРИТИХ КЛЮЧІВ УКРАЇНИ

Широке розповсюдження цифрових технологій та електронного документообігу потребує глобальної стандартизації протоколів взаємодії, зокрема засобів криптографічного захисту. Сертифікати відкритих ключів є невід’ємною складовою безпечної взаємодії в комп’ютерних мережах, їх використання включає побудову інфраструктури відкритих ключів (ІВК). Впровадження подібної системи потребує вирішення великого кола питань на різних рівнях роботи системи: від особливостей обладнання та криптоалгоритмів до нормативно-правової бази держави. Україна активно розвиває власну ІВК, базуючись як на міжнародних, так і на національних стандартах.

Більшість сучасних асиметричних криптосистем є вразливими до криптоаналізу з використанням квантового комп’ютера достатньої обчислювальної потужності, який може бути створений в найближчому майбутньому. З метою аналізу та стандартизації нових криптосистем NIST проводить відкритий конкурс. У першому раунді було представлено два алгоритми цифрового підпису (ЦП) на основі геш-функцій – SPHICS+ [1] і Gravity-SPHINCS, які є незалежними модифікаціями раніше розробленого алгоритму SPHINCS. До третього туру в якості альтернативного алгоритму пройшла тільки криптосистема SPHINCS+. В найближчі роки алгоритм SPHINCS+, можливо з деякими модифікаціями, може бути прийнято та стандартизовано на міжнародному рівні.

Метою даної роботи є проаналізувати структуру алгоритму SPHINCS+, оцінити можливість його використання в якості українського стандарту та побудови ІВК на його основі.

Загальна ідея підписів, що базуються на геш-функціях, полягає в тому, що у відповідність до повідомлення ставиться масив бітових рядків, елементи якого обрані та, можливо, прогешовані певну кількість разів, відповідно до бітів повідомлення. Клас підписів на основі геш-функцій включає велику кількість алгоритмів. Стійкість усіх алгоритмів цього класу ЦП базується на односторонній природі геш-функцій та їх стійкості до колізій.

Основними перевагами підписів на основі геш-функцій є постквантовість, легка модифікація, глибоко досліджена математична база. До недоліків слід віднести обмежену кількість підписів, що можуть бути створені за допомогою однієї пари ключів, та великі розміри підпису.

Найбільш перспективним ЕЦП на базі геш-функцій на даний час є сімейство алгоритмів SPHINCS. Загальна структура цих схем є однаковою, відрізняються деякі допоміжні алгоритми та деталі реалізації. Розглянемо цю групу алгоритмів на прикладі схеми SPHINCS+.

SPHINCS+ використовує структуру гіпердерева наступного вигляду: листям дерев Мерклі на усіх рівнях є геш-значення відкритих ключів підпису Вінтерніца. Ключі на нижньому рівні використовуються для підпису відкритих ключів FORS. Ключі FORS використовуються для підпису повідомлень. Ключі WOTS інших шарів використовуються для підпису коренів дерев шаром нижче. Підпис повідомлення являє собою підпис FORS, підписи коренів проміжних дерев, шляхи автентифікації.

Усі криптосистеми сімейства SPHINCS мають так звану віртуальну структуру: повне гіпер-дерево ніколи повністю не обчислюється, під час створення підпису обчислюється індекс FORS та генерується необхідний компонент гіпер-дерева – ланцюг, що включає по одному дереву на кожному шарі. Подібна конструкція фактично знімає обмеження на розмір гіпер-дерева, що буде використовуватись, і, відповідно, кількість підписів, що можуть бути безпечно створені з використанням однієї пари ключів.

Особистим ключем SPHINCS+ є дві випадкові бітові послідовності: одна разом з системою адресації дозволяє генерувати елементи гіпердерева; інша використовується для псевдовипадкового вибору індексу ключової пари підпису FORS, а відповідно і усіх проміжних дерев, що використовуються. Відкритим ключем є корінь дерева верхнього рівня та випадкова послідовність, що є додатковим джерелом ентропії під час проміжних гешувань.

Проведені розрахунки та експериментальний аналіз показали:

1) Генерація підпису SPHINCS+ для гіпердерева великих розмірів займає одиниці секунд; перевірка виконується за десятки мілісекунд.

2) Підписи SPHINCS+ мають великий розмір (десятки кілобайт), що обмежує їх використання у малоресурсній криптографії, зокрема, смарт-картах.

Діюча в Україні ІВК використовує алгоритм підпису на базі еліптичних кривих згідно ДСТУ-4145:2002. ІВК використовує ієрархічну структуру, що складається з таких основних компонентів [2]: центральний засвідчувальний орган (ЦЗО), засвідчувальні центри (ЗЦ) Центральних органів виконавчої влади, акредитовані центри сертифікації ключів (АЦСК), центри сертифікації ключів (ЦСК), відокремлені пункти реєстрації ключів, заявники – юридичні та фізичні особи (користувачі), контролюючий орган.

Впровадження ІВК для підтримки ЦП на основі геш-функцій не потребує змін щодо структури діючої інфраструктури. В контексті аналізу слід виділити три функціонально відмінні компоненти ІВК: ЦЗО, ЦСК та користувачі.

В якості базової функції гешування, яка фактично забезпечує стійкість усієї системи, може використовуватися алгоритм „Купина”. Вона підтримує різну довжину вихідного значення, що дозволяє використовувати її для забезпечення різних рівнів стійкості.

ВИСНОВКИ

Криптосистеми сімейства SPHINCS є багатокomпонентними та включають ряд параметрів, що дозволяють досягнути просторово-часового компромісу. Стійкість усіх ЕЦП на базі геш-функцій базується в першу чергу на однобічній природі геш-функцій та стійкості до колізій.

Попередній аналіз показав, що використання підписів SPHINCS+ в ІВК потребує конкретизації ряду параметрів, зокрема, необхідної висоти гіпердерева, рішення цієї проблеми потребує аналізу ймовірностей колізій при виборі підпису FORS, що буде використаний.

Побудова ІВК є комплексним процесом, що вимагає вирішення низки задач. Існуюча в Україні система ЦП може бути адаптована під використання будь-якої математичної бази, зокрема криптографії на базі геш-функцій. Впровадження системи з використанням ЦП подібного до SPHINCS+ включає два головних етапи: стандартизація криптоперетворень та модифікація існуючої ІВК. Обидва етапи потребують значних матеріальних витрат та часу. Однак, впровадження постквантового алгоритму ЦП на державному рівні є важливим кроком для національної кібербезпеки.

Подальші дослідження будуть спрямовані на програмне моделювання описаних алгоритмів та основних компонентів ІВК з використанням алгоритму SPHINCS+.

ЛІТЕРАТУРА

1. Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Andreas Hulsing, Panos Kampanakis, Stefan Kolbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, and Peter Schwabe. SPHINCS+ – Submission to the NIST’s post-quantum cryptography standardization process, 2019.

2. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика. Харків : Форт. 2010. 593 с.

КРИПТОГРАФІЧНІ АЛГОРИТМИ НА ОСНОВІ БАГАТОВИМІРНИХ КВАДРАТИЧНИХ ПЕРЕТВОРЕНЬ ЯК КАНДИДАТИ НА РОЛЬ ОСНОВНИХ У ПОСТКВАНТОВИЙ ПЕРІОД

Аналіз показав, що США на рівні NIST, Європейський Союз на рівні ETSI, Японія та Німеччина розпочали активну роботу по формуванню вимог до квантово-захищених криптоалгоритмів. Так до кінця 2026 року планується в основному розробити та розпочати відкрите обговорення квантово-захищених алгоритмів [1 – 4]. За результатами вказаних робіт будуть запроваджені нові криптографічні стандарти для постквантового періоду.

Ставиться задача дослідити процеси аналізу та розробки перспективного криптографічного перетворення типу цифровий підпис (ЦП) Rainbow, виявити його здатності відповідати вимогам щодо стандартизації для застосування у перехідний та постквантовий періоди. Метою цієї доповіді є аналіз сутності та застосування теорії та практики MQ-криптоперетворень стосовно ЦП Rainbow, визначення деталей специфікації механізму, базовий та формальний опис алгоритмів та функцій, що необхідні для реалізації механізму ЦП Rainbow, а також обґрунтування та розробка пропозицій щодо побудування та застосування наборів параметрів механізму ЦП Rainbow.

Багатовимірні квадратичні перетворення є криптографічними, якщо при їх виконанні застосовуються спеціальні дані – асиметричний ключ. Він складається з відкритого ключа K_e та особистого (таємного) K_o . Основною вимогою до асиметричної пари (K_e, K_o) є вимога, щоб $K_e \neq K_o$ та, щоб при знанні одного із них – наприклад, як на практиці – відкритого, визначення таємного було експоненційно складним. Як мінімум в деяких випадках – суб'експоненційно складним. Відкритий ключ K_e будується із поліномів скінченного поля P . На практиці це завжди сукупність коефіцієнтів p_i 's, що складаються (розміщуються) у певному порядку. Це робиться з метою зменшення складності обчислень. Так як K_e є відкритий ключ, то $P(0)$ завжди дорівнюється нулю.

Таємний ключ складається з інформації, що міститься в S, TiQ . Тобто, складається з $(M_S^{-1}, c_S), (M_T^{-1}, c_T)$ та усіх параметрів, які існують в Q . Теоретично, один з c_S та c_T може бути зайвим, але він зберігається у будь-якому випадку.

Для того, щоб перевірити підпис або зашифрувати інформацію направлено, застосовується відкритий ключ у вигляді $z = P(w)$.

Для того, щоб підписати або розшифрувати, застосовується таємний ключ у вигляді $y = T^{(-1)}(z)$, $x = Q^{-1}(y)$ і $w = S^{-1}(x)$. Але потрібно зважити на те, що це може бути тільки один з багатьох прообразів, який не обов'язково являється зворотною функцією у змісті криптографічного перетворення.

Необхідно відмітити, що навіть, якщо ми обмежимося криптосистемами, для яких відкритий ключ являє собою набір поліномів $P = (p_1, \dots, p_m)$ у змінних $w = (w_1, \dots, w_n)$, де всі змінні і коефіцієнти знаходяться в $K = F_q$, шлях, який приховує перетворення (можливо лазівку) не є унікальним. Проте, повідомлення завжди можна захистити за допомогою афінних перетворень S, T . Тобто, $P = T \circ Q \circ S : K^n \rightarrow K^m$.

Також необхідно відмітити, що у будь-якому перетворенні головне перетворення Q належить до певного класу квадратичних відображень, при чому для нього зворотне перетворення з точки зору складності виконання є поліноміально складним. При цьому таємні відображення S та T є афінними (можливо навіть лінійними) та повного рангу. В цьому випадку x_j називається центральною змінною, а поліноми y_i та x називаються центральними поліномами. Далі, коли необхідно знайти різницю між змінною та значенням,

то її позначають як $y_i = q_i(x)$. При цьому ключ K_C є основою такого механізму. Також наведемо позначення, які використовуються далі. Розмір блоку шифру або набору повідомлень – m елементів F_q . Блок відкритого тексту або розмір підпису – n елементів в

скінченному полі F_q . Розмір відкритого ключа $\frac{mn(n+3)}{2}$, F_q – елементи, які зберігаються.

Розмір таємного ключа оцінюється як $(n^2 + m^2 + [\text{\#параметри в } Q])$.

F_q – елементи, які зберігаються у відповідному форматі.

Складність таємного перетворення оцінюється як $(n^2 + m^2)$.

Складність відкритого перетворення з наближенням можна оцінити як $mn^2 / 2F_q$.

Трудомісткість (складність) генерації ключа – n^2 в полі F оцінюється в інтервалі $(O(n^4) - O(n^5))$.

Попередній аналіз дозволив виявити основний недолік багатовимірних перетворень – суттєве збільшення, у порівнянні з традиційними криптосистемами RSA, DSA або ECC, довжини ключів. Але вказане, як і інші питання властивостей багатовимірного перетворення та умов його застосування, вимагають непростих досліджень.

Загальна характеристика MQ-систем полягає в тому, що вони дозволяють в залежності від вимог, змінювати, наприклад:

- розмір ключа та час генерації;
- розмір підпису та час генерації;
- розмір ключа та збільшення розміру повідомлення.

MQ-схеми ЦП досліджувались вже два десятиліття до нашого часу. Теорія – розроблена на достатньому рівні. Наразі важливою є проблема переходу від теорії до практичної реалізації ефективних ЦП.

Таким чином, MQ-перетворення витримали випробовування більш, ніж 3 десятиліттями. Процес вироблення ЦП Rainbow складається з простих алгебраїчних лінійних операцій, таких як множення матричного вектору та розв'язування лінійних систем над невеликими кінцевими полями. Схема Rainbow має суттєві переваги та перспективу. В схемі Rainbow використовуються змінні *vinegar* та *oil* (v та o). Основними для безпечної схеми є параметри: $n = v + o$ та $v = 2o \dots 3o$. У цьому випадку $o = m$.

Підписи, вироблені з використанням схеми Rainbow, мають невеликий розмір, лише кілька сотень біт і тому набагато коротші, ніж інші постквантові ЦП.

ЦП Rainbow не вимагає складних обчислень. Це пояснюється тим, що Rainbow вимагає лише простих лінійних операцій з алгеброю над невеликими кінцевими полями. Вказане може бути ефективно застосовано на пристроях з низькою вартістю. Схема ЦП Rainbow реалізується на базі MQ багатовимірних перетворень. Вона базується на схемі Oil та Vinegar. Сутність таких схем полягає у тому, що існують два типи змінних – *vinegar* та *oil*. Перші при обчисленні центрального відображення обираються випадковим чином, а другі використовуються як значення геш-функції від повідомлення. В процес першого етапу конкурсу NIST автори ЦП Rainbow вдосконалили алгоритм генерації ключів, який було подано у пропозиції першого туру. Щоб прискорити процес генерації ключів Rainbow, автори перейшли від обчислення відкритого ключа шляхом інтерполяції до обчислення відкритого ключа за допомогою матриць.

ГЕНЕРАЦІЯ ЗАГАЛЬНОСИСТЕМНИХ ПАРАМЕТРІВ ДЛЯ СХЕМИ ЦИФРОВОГО ПІДПISY DILITHIUM ДЛЯ 5-7 РІВНІВ БЕЗПЕКИ

Однією з задач сучасної криптографії є пошук криптографічних схем, що є стійкими до атак на квантових комп'ютерах. Наразі триває третій етап відкритого конкурсу NIST PQS, однією з цілей якого є прийняття стандартів нових перспективних постквантових підписів. До третього етапу переважно пройшли підписи на алгебраїчних решітках, одним з яких є схема Dilithium. Отже, вивчення умов за яких схема забезпечує заданий рівень безпеки є актуальною задачею.

Метою роботи є дослідження умов за яких схема цифрового підпису (ЦП) Dilithium забезпечує потрібний рівень криптографічної стійкості та генерація наборів загальносистемних параметрів для 5-7 рівнів безпеки.

Для генерації загальносистемних параметрів в першу чергу необхідно провести аналіз відомих атак на криптосистему та встановити умови за яких забезпечується захист від них. Найочевиднішим вектором атаки криптосистеми є відновлення закритого ключа з відкритого ключа. В криптосистемі Dilithium вирішення цієї задачі зводиться до задачі MLWE (Module learning with errors). В літературі для аналізу MLWE використовується стратегія зведення до проблеми LWE, відома як „Core-SVP”. З математичної точки зору не відомо, чи можлива редукція проблеми Module-LWE до LWE, проте серед науковців поширена думка, що така редукція є малоімовірною. Зведення MLWE до LWE робиться з припущення, що не відомо атак з використанням алгебраїчної структури поліноміальних кілець для редукції решітки. Наразі це фактично єдиний відомий підхід для оцінки криптостійкості. З однієї сторони це полегшує аналіз, але з іншої залишає простір для оптимізацій. Методика Core-SVP враховує тільки атаки з використанням редукції решіток. Проте існують альтернативні атаки. Найбільшою категорією альтернативних методів криптоаналізу є комбінаторні атаки, такі як BKW, Arora-Ge та зустріч посередині. Ефективність атак цього класу залежать переважно від коефіцієнтів вектору поліномів, що є секретним ключем. Такі атаки мають сенс, коли коефіцієнти належать до фіксованої множини малого розміру (як правило $\{-1, 0, 1\}$). У схемах цифрового підпису така умова не часто виконується. На практиці їх використання має місце тільки для аналізу гомоморфних криптосистем. Тож, під час генерації загальносистемних параметрів потрібно врахувати, щоб при семплуванні поліномів секретного ключа використовувався розподіл з достатньо великою дисперсією. Основним засобом криптоаналізу є атаки з використанням редукції решіток. Можливо використовувати не тільки LWE-решітку, але і дуальну відносно неї. LWE-решітку часто задають як

$$\Lambda = \{x \in \mathbb{Z}^{m+n+1} : (A | I_m | -c) * x = 0 \bmod q\}. \quad (1)$$

Тобто використовується підхід із зведенням до USVP і подальшою редукцією базису. При застосуванні цього методу для оцінки криптостійкості загальносистемних параметрів існує два основних підходи для отримання конкретних оцінок. Перший підхід полягає у застосуванні симулятора BKZ, за допомогою якого підбираються оптимальні параметри редукції. Альтернативою є використання ряду евристик для оцінки блоку редукції.

Оцінка складності редукції решітки для конкретного набору загальносистемних параметрів фактично зводиться до пошуку розміру блоку редукції b для BKZ. Знайти його можливо з наступного співвідношення

$$\sigma \sqrt{b} \leq \delta_0^{2b-d-1} q^{\frac{n}{d}}, \quad (2)$$

де σ, q – загальносистемні параметри, d – розмірність решітки, δ_0 – максимальне значення фактора Ерміта, за якого решітка стає достатньо редукованою. δ_0 можливо виразити через b як:

$$\delta \approx \left((\pi b)^{\frac{1}{b}} * b / 2\pi e \right)^{1/2(b-1)}. \quad (3)$$

Вираз (2) представляє собою нелінійне Діафантове рівняння. Існує багато шляхів його вирішення, проте, оскільки, значення блоку редукції приймає достатньо малі значення, то можливо застосувати повний перебір.

Розглянемо атаку на дуальній решітці. Одним з способів завдання дуальної решітки є

$$\hat{L} = \{(x, y) \in \square_q^m \times \square_q^n \mid A^* x = y \bmod q\}. \quad (4)$$

У цьому випадку можливо вирішити задачу Decision-LWE за допомогою зведення до SIS. При криптоаналізі потрібно встановити чи належить вектор, що отриманий з використанням редукції на цій решітці, до LWE-розподілу, або рівномірного розподілу. Ймовірність вдалого пошуку визначається статистичною відстанню між цими двома розподілами. Оцінити відстань можливо як:

$$\varepsilon = 4 \exp \left(-2\pi^2 \left(\frac{l\sigma}{q} \right)^2 \right), \quad (5)$$

де l – довжина найменшого вектора. Відповідно, потрібно перебрати $1/\varepsilon$ редукованих векторів, але практичні експерименти дають оцінку $1/\varepsilon^2$ таких векторів для вдалої атаки. Нехай вирішувач працює за час T , тоді кількість спроб можливо розрахувати як

$$R = \max \left(1, \frac{1}{T * \varepsilon^2} \right). \quad (6)$$

Оскільки довжина вектора l залежить від фактора Ерміта як $\delta_0^{d-1} q^{\frac{n}{d}}$, а той може бути виражений через розмір блока як (3), то задача знову зводиться до перебору значень параметра b . На основі стійкості до даних атак були знайдені загальносистемні параметри для 256, 384 та 512 біт безпеки.

Ймовірність повтору циклу при цьому складає для 256 біт – 0.15442678312246608, для 384 біт – 0.15609624568669475 і для 512 біт – 0.15247678668181552.

Таблиця 1

Загальносистемні параметри для 256, 384, 512 біт стійкості для схеми Dilithium

Набір	N, q	γ_1	γ_2	k, l	η	β	d	h	ω
256	(256, 8380417)	523776	261888	(9,8)	2	144	14	60	184
384	(512, 8380417)	523776	261888	(7,5)	5	100	13	77	286
512	(512, 8380417)	523776	261888	(9,8)	2	74	13	118	368

В даній роботі були знайдені загальносистемні параметри для схеми постквантового цифрового підпису Dilithium, що забезпечують 256, 384, 512 біт безпеки. Для оцінки криптографічної стійкості були використані атаки на LWE-решітці та дуальній до неї в межах методології Core-SVP.

Було встановлено, що безпеку можливо збільшувати двома шляхами. Перший полягає у збільшенні параметрів поля, другий полягає в збільшенні параметрів LWE.

Другий спосіб є більш перспективним з практичної точки зору, оскільки дозволяє значно збільшити безпеку без значних змін в реалізації.

ПІДСИСТЕМА ВИВЧЕННЯ ТА ВИЗНАЧЕННЯ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНИХ СИСТЕМ УМОВНОГО ПРОТИВНИКА.

Актуальність Проаналізувавши велику кількість програм для аналізу мережевих портів, можна зробити висновок про те, що всіх їх можна поділити на дві категорії: платні та ті, що знаходяться у вільному доступі. Крім того, переважна більшість програм, які відносяться до кожної із зазначених категорій, побудовані на основі закритого коду, що робить неприйнятним їх використання у системах спеціального призначення (зокрема, у військовій сфері) з огляду на неможливість гарантування безпеки передачі інформації.

Ще одна важлива особливість програм для аналізу безпеки мережевих портів – це їх точність. Наприклад, програми, що є у вільному доступі, мають можливість швидкого сканування визначеного діапазону портів, однак висока швидкість сканування дуже часто призводить до «втрати» портів, відображаючи їх як «закриті», хоча насправді ці порти можуть бути відкритими і нести в собі потенційну загрозу безпеки мережі.

Враховуючи зазначене, завдання розробки програмного забезпечення для сканування мережевих портів, яке б давало можливість змінювати програмний код та характеризувалося вищими показниками точності, у порівнянні з існуючим програмним забезпеченням із закритим кодом, є актуальним на сьогоднішньому етапі розвитку телекомунікаційних мереж військового призначення.

Мета дослідження є розробка програми для аналізу мережевих портів з відкритим кодом для застосування в мережах військового призначення ЗС України.

Виклад основного матеріалу сканер мережевих портів – програмне забезпечення, створене для виявлення хостів мережі, в яких відкрито потрібний порт або набір портів. Сканери портів, як правило, використовуються системними адміністраторами для виявлення слабких місць їх мереж. Їх використовують як хакери так і мережеві адміністратори. Сканер портів є дуже корисною утилітою, оскільки під час змін у своїй мережі адміністратор може забути порти, які він відкривав, для тих або інших змін і цим можуть скористатися зловмисники. Проникнувши через незакритий порт зловмисник може без проблем вчинити будь-які деструктивні дії щодо системи, у яку він проник. Якщо розглянути це з точки зору військової сфери то таке проникнення може спричинити несанкціонований доступ до закритої інформації, її викрадення чи знищення і, як наслідок, призвести до серйозних наслідків ведення бою або цілої війни. Враховуючи особливості застосування у військовій сфері, сканери портів повинні відповідати наступним вимогам: мати відкритий код для можливості покращення програми та збільшення її безпеки; не створювати навантаження на систему для уникнення перевантаження пристроїв з низькими технічними характеристиками апаратного забезпечення; забезпечувати належний рівень швидкості сканування для адекватного реагування на можливий напад.

Висновки. Отже, сканер портів, написаний на мові програмування високого рівня Python, може використовуватись на більшості пристроїв, має вищу точність сканування та менше навантажує пристрій, на якому він запущений. Все це свідчить про те, що програма має значний потенціал і перспективу до застосування при діагностиці мереж спеціального призначення, зокрема, у військовій сфері. Застосування запропонованої в роботі програми дозволить в повній мірі уникнути використання програм із закритим кодом, які є в мережі Інтернет, а її подальше удосконалення на основі мови програмування Python, як елементу для написання закритого програмного забезпечення, дозволить значно підвищити безпеку мережевої інфраструктури, що є особливо актуальним завданням у ході проведення сучасних інформаційних війн.

МЕТОД РОЙОВОГО УПРАВЛІННЯ ТАКТИЧНИМИ БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ

Проведений аналіз технічної літератури щодо використання збройними силами провідних країн світу безпілотних літальних апаратів (БПЛА) показав високу ефективність їх застосування під час проведення розвідки та проведення бойових операцій в зонах конфлікту. Безпілотні літальні апарати можуть бути використані військовими для різних цілей, таких як розвідка, виявлення ворожої техніки, живої сили противника тощо. БПЛА є найбільш перспективним напрямком розвитку авіації. Це пояснюється не тільки тим, що масове виробництво і застосування БПЛА виявляється дешевше і простіше, ніж пілотовані літальні апарати, але і тим, що деякі типи БПЛА спроможні вирішувати завдання, недоступні пілотованим літальним апаратам, наприклад, завдання ближньої розвідки в умовах щільної міської забудови. Пошкодження БПЛА в ході виконання бойової задачі несе лише фінансові втрати і не загрожує життю пілота-оператора, що дозволяє використовувати БПЛА в ризикованих операціях. **Від одиночних БПЛА до груп і комплексів.** Залежно від типу управління безпілотні літальні апарати поділяють на некеровані, дистанційно-пілотовані і автономні. Довгий час основну частину БПЛА становили дистанційно-пілотовані апарати. Ройова взаємодія – як одне з рішень проблем малорозмірних БПЛА. Однією з серйозних проблем, що стоять на шляху використанні малорозмірних БПЛА є проблемою в забезпеченні радіозв'язку з операторським пультом управління. Справа в тому, що малі розміри накладають суттєві обмеження на запас бортового енергоресурсу, велика частина якого призначена для забезпечення руху, і лише невелика частина енергоресурсу може використовуватися приймально-передавальною апаратурою. Таким чином, потужність радіо передатчиків сильно обмежена. Невеликі розміри БПЛА також обмежують розміри антен. Використання груп БПЛА робить питання забезпечення зв'язку ще більш актуальним. При централізованих стратегіях управління кожному БПЛА потрібен канал зв'язку з пропускнуою здатністю в кілька Мбіт/с для передачі зображення та іншої інформації про навколишнє середовище. Частковим рішенням проблеми може стати застосування централізованих ієрархічних стратегій управління, при яких зв'язок з центральним пристроєм управління є лише у деяких БПЛА, кожен з яких передає команди апаратам своєї підгрупи, причому дистанція між апаратами підгрупи відносно невелика, а звідси слідує, що енергозатрати на таку передачу не такі суттєві. В якості вирішення проблеми інформаційного обміну в групах БПЛА пропонується використовувати метод ройового інтелекту. Ройовий інтелект – це дисципліна, яка вивчає природні та штучні системи, що складаються з великої кількості окремих об'єктів, які здійснюють децентралізоване управління на основі принципів самоорганізації. Ройовий інтелект описує колективну поведінку децентралізованої самоорганізовуючого, природного або штучного походження. У групі БПЛА, яка взаємодіє на основі ройового інтелекту, кожен апарат здійснює взаємодію лише з деякими, найближчими до нього в даний час, апаратами. При цьому дальність зв'язку і енергозатрати на інформаційну передачу відносно невеликі. БПЛА приймають рішення в момент виконання завдання, спираючись на самостійно зібрані данні про навколишнє середовище, а також на ті дані, які передають сусідні апарати. Енергозатратний зв'язок з центральним пристроєм управління здійснюється лише зрідка, і взагалі не всіма апаратами групи, лише для того, щоб отримати інформацію про завдання, що стоять перед групою, і для того щоб передати звітну інформацію про стан групи і під час виконання поставленого раніше завдання. Недоліком існуючих методів ройового управління для тактичних БПЛА які виконують бойові завдання за призначенням є складність програмного забезпечення, бо малі розміри БПЛА накладають обмеження в бортовому обладнанні. Тому для зв'язності групи (рою) БПЛА пропонується представити розміщення в просторі БПЛА за допомогою просторової решітки для формування строю (БПЛА) під час виконання бойового завдання, які можуть виявитися найбільш ефективними.

CISCO SECUREX – ЕФЕКТИВНЕ РІШЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА СЕРВЕРНИХ ДОДАТКІВ

Ефективність управління військами (силами) передбачає: безперервне добування, збір, вивчення, відображення та аналізування даних про обстановку; прийняття рішення щодо планування та ведення операції (бою); доведення задач підпорядкованих військ (сил); організацію та підтримки взаємодії органів військового управління; організацію та проведення заходів із всебічного забезпечення підпорядкованих військ (сил).

Управління військами (силами) забезпечується за допомогою обміну інформацією між органами військового управління (вищими, підпорядкованими та взаємодіючими).

З метою прискорення обміну та підвищення якості обробки інформації, в органах військового управління розгорнуті інформаційні (автоматизовані) системи, об'єднані в єдину інформаційно-телекомунікаційну мережу. У зв'язку з цим виникає потреба в захисті інформації, що циркулює в інформаційнотелекомунікаційній системі (мережі), та необхідність у проведенні заходів із її безпечного функціонування.

Одним із таких інструментів є програмна платформа Cisco SecureX. Програмна платформа Cisco SecureX працює як багатокористувальницький вебдодаток (через браузер), забезпечує інтеграцію сервісів безпеки окремих серверних і мережових додатків та операційної системи в єдине середовище, а також виявляє причинно-наслідкові зв'язки загроз (інцидентів) в автоматизованому режимі. Інтеграція сервісів безпеки досягається за рахунок застосування розробниками лінійного інтерфейсу, який відображає журнали безпеки окремих додатків на одному екрані (вкладці) або панелі інструментів (dashdoard). Відображення зазначених журналів на одному екрані (вкладці) або панелі інструментів (dashdoard) дають змогу зменшити розсіяність уваги адміністратора безпеки інформаційної (автоматизованої) системи значно та підвищити якість сприйняття інформації цим адміністратором.

Автоматизація функцій інформаційної безпеки системи досягається за рахунок наявності інструментарію формування відповідних запитів з інтегрованих джерел даних та візуалізації їх результатів.

Якщо адміністратор встановлює рівень індикатора загрози (граничного показника переходу кількісного показника в якісний), то програмна платформа Cisco SecureX сповіщає адміністратора про загрозу (інцидент) і/або автоматично реагує на неї (нього). Наявний у платформі інструментарій побудови логічних конструкцій (алгоритмів) дає змогу виявляти причинно-наслідкові зв'язки загроз (інцидентів) та будувати мережові граfi і теплові матриці їх активності в автоматичному режимі. Застосування програмної платформи Cisco SecureX при адмініструванні інформаційних (автоматизованих) систем дозволяє підвищити їх рівень стійкості та живучості.

Основною вимогою функціонування програмної платформи Cisco SecureX є використання серверного та комутаційного обладнання компанії Cisco.

Застосування цієї платформи в інформаційних (автоматизованих) системах розгорнутих в органах військового та державного управління цілком можливе, але за умови проведення циклу випробувань та отримання на неї позитивного експертного висновку і/або атестату відповідності, виданого Адміністрацією Державної служби спеціального зв'язку та захисту інформації України.

УДОСКОНАЛЕНИЙ МЕТОД КООРДИНАТНОЇ МАРШРУТИЗАЦІЇ В МОБІЛЬНИХ РАДІОМЕРЕЖАХ З НАПРАВЛЕНИМИ АНТЕНАМИ

Перспективним напрямком підвищення ефективності функціонування мобільних радіомереж (МР) класу MANET є застосування адаптивних антенних решіток. Антенні решітки з круговим розташуванням елементів (КАР) мають кращі характеристики, порівняно з лінійними. Для МР з КАР, враховуючи необхідність забезпечити знання кожним вузлом мережі координат (або просторового напрямку) сусідніх вузлів, найбільш перспективним є застосування методів координатної маршрутизації, основною перевагою яких порівняно з методами, що не використовують координатну інформацію, є значне зменшення обсягу службового трафіку.

При розробці методу КМ для МР з КАР необхідно вирішити наступні завдання: збір інформації про стан мережі; зберігання маршрутів; обчислення маршруту передачі пакету (визначення правил вибору одного чи декількох вузлів-ретрансляторів).

Реалізація збору інформації про стан мережі можлива хвильовим, зондовим або проактивним способами, а також гібридним, який передбачає, що кожен вузол мережі збирає інформацію про координати сусідніх вузлів на глибину маршрутної зони $R_{мз}$ проактивно, а за її межами – зондовим способом. Вибір конкретного способу може залежати від розмірності мережі, вимог до величини затримок при побудові маршруту тощо.

Зберігання маршрутів при координатній маршрутизації передбачає підтримання кожним вузлом таблиці місцезнаходження сусідніх вузлів наступного формату: ідентифікатор адресата j , його координати $(x, y, z)_j$, швидкість переміщення v_j , напрямок переміщення γ_j , час оновлення даної інформації t_j . Крім цього, необхідно обрати спосіб зберігання інформації про місцезнаходження – автономний (кожен вузол ініціює процес збору інформації про стан мережі та зберігає у своїй маршрутній таблиці) або розподілений (передбачає призначення деяких вузлів домашніми агентами, які відповідають за зберігання інформації про місцезнаходження тих чи інших вузлів).

Вибір ретранслятора полягає у визначенні напрямку пошуку адресата та визначенні розмірів зони його передбачуваного знаходження. Обчислення маршруту може бути реалізовано декількома способами: випадково з обмеженням вибору за певними правилами (наприклад, у прямокутній області певного розміру), або фіксований вибір ретрансляторів.

Застосування КАР потребує урахування даних про систему РЕП противника та прогнозування змін сигнальної та завадової обстановки з урахуванням даних про переміщення вузлів мережі один відносно одного та постановників завад.

При зміні координат на деяку величину ΔX j -го вузла (або постановника завад відносно нього) рівень сигналу i -го вузла ($i = 1, \dots, n$, де n – кількість вузлів у зоні радіовидимості вузла j) на вході приймача j -го вузла P_{ij} при взаємній орієнтації антен одна на одну зміниться незначно, у той же час, оскільки форма ДН КАР (інтенсивність та напрямки бічних та заднього пелюстків) суттєво залежить від напрямку основного випромінювання, рівень завади P_{zj} на вході приймача може суттєво зрости, порівняно з попереднім положенням. Відповідно, відношення сигнал/(завада + шум) (ВСШЗ) на вході приймача j -го вузла стане значно меншим. Враховуючи те, що сусідніх вузлів у j -го вузла може бути декілька, розрахунок очікуваного ВСШЗ $_{ij}$ після зміни координат на ΔX доцільно здійснювати сусіднім вузлам, для чого вони повинні знати його оновлені координати (або просторовий напрямок) та рівень завади на вході приймача у точці X_j .

Таким чином, після оновлення даних в таблиці місцезнаходження сусідніх вузлів, кожен вузол, який є сусідом j -го вузла, здійснює розрахунок максимально можливого ВСШЗ $_{ij}$, яке можна забезпечити шляхом керування направленістю випромінювання КАР.

ПЕРСПЕКТИВИ ПОБУДОВИ ГЕТЕРОГЕННИХ ІНФОРМАЦІЙНИХ СИСТЕМ ВОЕННОГО ПРИЗНАЧЕННЯ З УРАХУВАННЯМ КОНЦЕПЦІЇ NGN (NEXT GENERATION NETWORKS)

З метою забезпечення інформаційного обміну в гетерогенних інформаційних системах воєнного призначення використовуються багаточислені програмно-апаратні засоби, які дозволяють користувачам здійснювати обмін будь-якими видами повідомлень (голос, відео, передача даних), отримувати інформаційні послуги в будь-який час, в різних умовах обстановки із заданою якістю. Засоби інформаційних систем також дозволяють уніфікувати процедури надання доступу до інформаційних послуг для різноманітних користувачів, а також організувати міжмережну взаємодію з користувачами інших мереж.

Гетерогенні інформаційні системи воєнного призначення, в тому числі системи передачі даних, створюються на основі принципів побудови розподілених обчислювальних мереж, в яких на окремих об'єктах розгорнуті локальні обчислювальні мережі, які об'єднують автоматизовані робочі місця для виконання задач збору, обробки, зберігання та відображення інформації, які створені на базі виокремлених та арендованих телефонних каналів (IP телефонія), телеграфних каналів, радіорелейних, тропосферних та супутникових каналів передачі інформації.

Існує тенденція до створення середовища обміну інформацією на основі NGN. В данному напрямку стрімкого розвитку набувають інформаційні системи воєнного призначення США, в яких прийняті концептуальні рішення по об'єднанню в єдиний інформаційний простір різноманітних мереж та систем зв'язку, з переходом до персоналізованих послуг зв'язку для кожного абонента без залежності від його місця розташування.

Слід розглянути, що розуміється під NGN так, як саме поняття NGN досі є досить неоднозначним. Під системами та технічними рішеннями NGN розуміються:

1. Транспортні мережі NGN на основі MPLS/IP або GFP/SDH
2. Системи абонентського доступу ADSL, G.SHDSL, ADSL2 + та Gigabit Ethernet.
3. Системи комутації нового покоління засновані на SoftSwitch.
4. Підсистеми верхнього рівня: інформаційні системи, системи зберігання інформації (SAN), системи забезпечення безпеки і т.д.

Основу мережі NGN складає мультипротокольна телекомунікаційна система (як правило, на основі ATM, IP, MPLS), яка надає послуги транспортування і реалізує функції транспортного рівня і рівня управління викликами. Метою побудови транспортної мережі NGN є перехід від окремих мереж попереднього покоління, призначених для окремих груп користувачів або послуг (телефонія, дані та ін.) до інтегрованої мережі з гарантованою якістю обслуговування.

Концепція NGN передбачає створення регіонального та магістрального сегментів мережі. При цьому на регіональному рівні має забезпечуватися підключення користувачів і надання їм транспортних послуг, а також взаємодія з аналогічними регіональними транспортними мережами. На магістральному рівні повинне забезпечуватися надання послуг перенесення конвергентного трафіку для взаємодії регіональних мереж, а також для передачі трафіку всіх існуючих мереж.

Даний підхід забезпечить подальше підвищення ефективності використання мережних ресурсів при впровадженні NGN за рахунок об'єднання різних телекомунікаційних систем фіксованого та мобільного зв'язку в складі гетерогенних інформаційних систем воєнного призначення в єдину транспортну мережу IP/MPLS, яка підтримує широкий спектр технологій доступу.

ОСОБЛИВОСТІ ДІАГНОСТУВАННЯ ТА РЕМОНТУ ТЕХНІКИ ЗВ'ЯЗКУ В УМОВАХ ПРОВЕДЕННЯ БОЙОВИХ ОПЕРАЦІЙ

Одним з найважливіших напрямків організації експлуатації військової техніки зв'язку (ВТЗ) є діагностичне забезпечення. Сукупність принципів, методів і засобів пошуку несправностей становить основу діагностичного аспекту надійності, у рамках якого необхідно вирішувати завдання діагностування ВТЗ, тобто організація перевірки справності, працездатності, правильності функціонування засобів зв'язку і пошуку несправностей у них у процесі виробництва, експлуатації й ремонту. Узагальненим показником надійності є коефіцієнт готовності, що визначає імовірність того, що об'єкт виявиться працездатним в довільний момент часу, крім запланованих періодів, протягом яких застосування об'єкта по призначенню не передбачається. Проте, виникає істотна складність щодо прогнозування безвідмовної роботи в реальних умовах, особливо в умовах ведення бойових дій. Також відомо, що при досить великому обсязі статистичної вибірки значень наробітку на відмову та середнього часу відновлення окремих складових апаратури і зразків ВТЗ в цілому, статистичне значення коефіцієнта готовності наближається до дійсного значення.

Проте, у зв'язку із розвитком переоснащення апаратних зв'язку новітніми засобами, та відсутністю можливостей бойових підрозділів проводити діагностування та ремонт такої техніки, стає практично неможливим прогнозування безвідмовної роботи систем зв'язку в цілому. Крім того, із розвитком елементної бази різномісних засобів зв'язку відомі методики технічного діагностування стають непристосованими до виконання задач діагностування ВТЗ, а засоби діагностування потребують удосконалення.

На сьогодні в Збройних Силах України (ЗСУ) існує трирівнева система технічного обслуговування і ремонту (СТОіР): рівень експлуатації (бойові підрозділи); військові ремонтні органи (штатні ремонтні підрозділи, бази ремонту); ремонтні підприємства.

Таким чином, територіальна віддаленість рівнів СТОіР приводить до збільшення середнього часу відновлення зразків ВТЗ, і як наслідок на коефіцієнт готовності.

З цих причин система технічної діагностики, стає менш ефективною, а в умовах проведення бойових операцій зовсім не може забезпечити необхідного рівня бойової готовності.

Отже, актуальність розробки нових методик діагностування та ремонту ВТЗ у ЗСУ визначається наступними обставинами:

- відсутність статистичної інформації про типові несправності;
- значна територіальна віддаленість рівнів СТОіР;
- діагностичне та вимірювальне обладнання апаратних технічного забезпечення не дозволяє провести діагностування та ремонт новітніх засобів зв'язку;
- значний час локалізації дефектних цифрових радіоелектронних компонентів (РЕК) ВТЗ (до 70 % від загального часу відновлення ВТЗ);
- необхідність виконання робіт по відновлюванню ВТЗ замість їх заміни новими;
- значні працезатрати, і як наслідок, вартість відновлювальних робіт.

Тому виникає потреба в розробці і використанні нових, відносно недорогих, адаптованих до сучасної елементної бази методів технічного діагностування та ремонту, та пристроїв, які дозволяють скоротити кількість контрольних точок і діагностичних параметрів (з урахуванням статистичної інформації про типові несправності), з метою зменшення часу на пошук і локалізацію дефектних РЕК сучасної ВТЗ.

Таким чином, перспективи розвитку СТОіР ВТЗ визначається необхідністю нового підходу, направлено на виконання вимог до часових і економічних показників відновлення працездатності.

ШЛЯХИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ КЛАСУ 1 В УМОВАХ ЗАСТОСУВАННЯ ПРОТИВНИКОМ ЗАСОБІВ ВОГНЕВОГО УРАЖЕННЯ.

В наш час, застосування безпілотних літальних апаратів, під час ведення збройної боротьби набувають актуальності вносячи особливий вклад у військову справу. Поряд з цим існують проблеми. Критерії ефективності планування маршруту польоту розвідувального БпЛА тактичної ланки обумовлюються:

- завданням вищого штабу;
- можливостями противника щодо зриву розвідувального завдання;
- часовими параметрами планування та (або) виконання місії;
- параметрами, які визначають технічні можливості БпЛАК.

Ще однією з головних проблем є протиповітряна оборона противника (ППО), перед якою стоїть задача по своєчасному виявленню і знищенню малорозмірних, тихохідних літальних апаратів. Задача оператора пілота безпілотного літального апарату (БпЛА) полягає в тому, щоб повністю зберегти літальний апарат без втрат ефективності його застосування.

З особливостей застосування ППО можна виділити:

- створення спеціальних груп, до складу яких входять зенітні формування;
- модернізація існуючих зразків зенітного озброєння;
- розробка перспективних зразків зенітного озброєння стосовно рішенням специфічних завдань щодо виявлення та ураження малорозмірних повітряних цілей;
- розробка спеціалізованих комплексів та засобів боротьби з малорозмірними цілями, заснованих на застосуванні нетрадиційних видів зброї.

Засоби протиповітряної оборони противника являються значною небезпекою для ефективності роботи БпЛА та виконання ними завдань за призначенням. В період ведення бойових дій на сході нашої країни, через засоби вогневого ураження противника, були зафіксовані втрати БпЛА.

Одним з підходів для вирішення даної проблеми може стати розробка алгоритму, який буде забезпечувати прокладання оптимального маршруту руху із урахуванням апріорної інформації із засобів космічної розвідки з попереднім визначенням ймовірних районів розташування ворожих засобів ППО та їх тактико технічних характеристик щодо небезпечних зон ураження, з відповідним відображенням такої обстановки на цифровій електронній карті на наземному пункті управління, що не лише полегшить роботу оператора пілота, який проводить побудову маршруту руху БпЛА а й дозволить спрогнозувати небезпечні зони його польоту.

В результаті проведених досліджень встановлено необхідність розробки математичної моделі, яка б забезпечувала:

- врахуванням вимог розвідувального завдання та умов протидії противника;
- використанням математичного апарату для планування маршруту польоту розвідувального БпЛА класу 1 з урахуванням основних факторів впливу зовнішнього середовища;
- оперативно визначати числові значення основних критеріїв планування маршруту польоту розвідувальних БпЛА тактичної ланки;
- визначати можливість застосування конкретного зразка БпЛА для виконання розвідувального завдання.

ЗАСТОСУВАННЯ ЗАСОБІВ МАШИННОГО НАВЧАННЯ В ІНФОРМАЦІЙНИХ (АВТОМАТИЗОВАНИХ) СИСТЕМАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

За нормативним визначенням, наведеним у статті 1 Закону України „Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994 № 80/94-ВР, інформаційною (автоматизованою) системою є організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

Сучасні інформаційні (автоматизовані) системи зберігають і обробляють великий обсяг структурованої та неструктурованої інформації. Тому для її оброблення актуальними є розроблення й застосування засобів машинного навчання.

Для якісного функціонування засобів машинного навчання слід розробляти й застосовувати алгоритми побудови нейронних мереж. Побудова таких мереж в інформаційних (автоматизованих) системах військового призначення дає змогу в автоматичному режимі виявляти та ранжувати серед наявної інформації асоціативні зв'язки (закономірності та/або аномалії) для оцінки дій угруповання противника та прийняття рішення при плануванні його вогневого ураження в операції (бою). Основною вимогою для функціонування цих алгоритмів є збір та накопичення статистичних даних про об'єкти дослідження. Для успішного функціонування алгоритмів побудови нейронних мереж в інформаційних (автоматизованих) системах військового призначення вихідними даними є:

- бойовий і чисельний склад угруповання противника та своїх військ (сил);

- перелік оперативних і тактичних нормативів застосування окремих елементів угруповання противника та своїх військ (сил);

- каталог об'єктів противника та своїх військ (сил), разом з їх властивостями й характеристиками;

- перелік типових сценаріїв для ведення сторонами операції або бою (оборона, наступ, контрнаступ, стабілізаційні дії, форсування тощо) з урахуванням історичного та бойового досвіду, а також вимог настанов і бойових статутів;

- статистика стану та положення угруповання противника та своїх військ (сил);

- картографічна основа для функціонування електронної карти місцевості.

За результатами роботи алгоритмів побудови нейронних мереж в інформаційній (автоматизованій) системі виявляються та ранжуються асоціативні зв'язки (закономірності та/або аномалії) з відповідними кількісними показниками.

Для пошуку асоціативних зв'язків (закономірностей та/або аномалій) зазвичай використовуються такі базові алгоритми (правила):

- Apriori* – визначення правила пошуку кількості транзакцій серед набору груп елементів;

- Lift* (підтримка) – встановлення рівня взаємозалежності елементів;

- Eclat* – визначення правила прискорення обрахунку транзакцій взаємодії елементів.

За умови надання кількісним показникам відповідних вагових коефіцієнтів та граничних показників переходу кількісного показника в якісний, система в змозі побудувати дерево прийняття рішень, яке є основою для вироблення висновків та прогнозування розвитку ситуації (події, явища). Побудоване засобами машинного навчання дерево прийняття рішень дає змогу більш точно оцінити наступальні можливості угруповання як своїх військ (сил), так і противника при досягненні ними суто військових цілей (глибина і тривалість наступу (оборони), оцінка його оперативних та військових резервів тощо). У разі прогнозування розвитку суспільно-політичної обстановки, побудоване засобами машинного навчання дерево прийняття рішень має ряд обмежень і носить усереднений характер, оскільки соціальні процеси досить важко формалізуються та не передбачають своєчасного врахування усіх людських (фізіологічних) й психологічних факторів осіб, що приймають.

МЕТОДИКА РЕАЛІЗАЦІЇ ДИНАМІЧНОЇ HONEYPOT-СИСТЕМИ НА ОСНОВІ КОНТЕЙНЕРНОЇ ВІРТУАЛІЗАЦІЇ

Поряд з традиційними методами захисту корпоративних мереж від вторгнень, такими як системи виявлення вторгнень (*IDS*) і системи запобігання вторгнень (*IPS*), існують і альтернативні підходи до забезпечення безпеки інформаційних ресурсів. Одним з таких підходів є використання технології *honeypot*. Одне з найсерйозніших завдань, яке доводиться вирішувати фахівцям з безпеки – це збір відомостей, що дозволяє виявити атаки, зрозуміти, яким чином відбуваються мережеві атаки, алгоритм їх дій та об'єкти посягання. Раніше суть кіберзагрози намагалися з'ясувати, виключно аналізуючи програми, використані для проникнення, після того як стався інцидент, єдині дані, на які могли розраховувати фахівці – це інформація, що залишилася у зламаній системі. На жаль, вона вкрай мізерна і мало що може сказати про загрозу в цілому. Для вирішення вищезазначених проблем має місце використання технології *honeypot*.

Honeypot – інформаційний ресурс системи, призначення якого полягає у встановленні неправомірного або незаконного використання ресурсу. Фактично це приманка, фальшивий об'єкт для атаки, який повністю знаходиться під контролем системи інформаційної безпеки, у вигляді імітації потенційно вразливого об'єкта з подальшим дослідженням дій зловмисника.

Honeynet – це мережа високорівневої взаємодії *Honeypot*, яка має здатність моделювати мережі і можливість контролювати зареєстрований, граничний і неправомірний доступ. Виявлення атак на основі мережевих приманок, зокрема *Honeypot*, дозволяє істотно розширити інформацію про атаку.

Використання даної системи забезпечує вирішення наступних задач:

- виявлення раніше невідомих проблем в інформаційній системі;
- вивчення покрокових дій зловмисника в інформаційній системі;
- збір інформації про використовувану інфраструктуру злочинця;
- виявлення раніше невідомого шкідливого програмного забезпечення;
- виявлення цілей, переслідуваних зловмисником, і потенційних об'єктів посягання.

Основні переваги використання контейнерної віртуалізації в методиці реалізації *honeypot*-системи:

- той факт, що адміністрування систем, керованих приманкою, потребує багато часу, мотивуючи використання контейнерів для спрощення їх управління;
- можливість приманок зіставляти події атаки, щоб визначити, чи є вони локалізованими або розподіленими, дозволяючи швидко ідентифікувати їх тенденції;
- використання контейнерів надає додатковий рівень оманливості: оскільки приманки є ізольованими середовищами, які спільно використовують ядро реальної операційної системи, вони з більшою ймовірністю будуть виглядати як реальна система при знятті відбитків системи.

Таким чином, *Honeypot* – це цінний інструмент для дослідження нових векторів атак і шкідливих програм. Технологія відмінно надає допомогу у ідентифікації та визначенні типів атак та вразливостей. Метою *Honeypot*-системи є зазнавання атаки або несанкціонованого дослідження, що дозволяє захистити дійсну систему методом перенаправлення дій зловмисника на імітовану приманку, крім того це дозволяє запротоколювати процес атаки, що згодом дозволить вивчити стратегію зловмисника та визначити перелік засобів та алгоритмів, за допомогою яких можуть бути завдані удари реально наявним об'єктам безпеки. Реалізація *Honeypot* може бути спеціальним виділеним сервером, або мережевим сервісом, завдання якого, базується на приверненні уваги зловмисника та наданні йому хибного розуміння того, що його дії вірні.

ПОРЯДОК АВТОМАТИЗОВАНОГО ЗАБЕЗПЕЧЕННЯ ДАНИМИ ПРО МЕТЕОРОЛОГІЧНІ УМОВИ, ДЛЯ ЕФЕКТИВНОГО ВИКОРИСТАННЯ БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ І КЛАСУ

Безпілотні літальні апарати (БпЛА) все частіше застосовуються у військовій справі, в першу чергу для ведення повітряної розвідки. Для успішного виконання завдань зовнішньому пілоту (оператору) БпЛА варто своєчасно отримати та чітко розуміти метеорологічні умови, за яких виконується політ, адже вони впливають на усі етапи польоту БпЛА, а значить і на можливість виконання бойового завдання та хід ведення бойових дій.

Основною особливістю підготовки операторів БпЛА є те, що необхідно не тільки навчити керувати ним, а й застосовувати набуті компетенції для успішного виконання бойових завдань, а саме з оцінювання метеообстановки. Важливим напрямом забезпечення безпеки польотів є аналіз загрози успішному виконанню професійних завдань з участю БпЛА за допомогою класифікації типів хмар, зокрема її поєднання з характером вертикальних рухів і висот виникнення з додатковою складовою – можливістю опадів. На сьогодні використовується морфологічна міжнародна класифікація хмар. Вона включає 4 родини (яруси), 10 родів (форм), 20 видів та 35 різновидів, які відрізняються за умовами утворення, структурою, щільністю, забарвленням, характером опадів, оптичними явищами тощо. Оператор за зовнішнім виглядом хмар повинен прийняти правильне рішення про виконання польоту, його характер і посадку БпЛА з метою виконання поставленого бойового завдання та збереження самого апарата. Таким чином, оператор БпЛА повинен розуміти та вміти використовувати метеорологічну інформацію, визначати небезпечні явища погоди, забезпечувати безпечний прохід фронтальних зон і обхід небезпечних метеоумов.

Інтенсивна турбулентність, сильний вітер, опади, обмерзання можуть значно ускладнити або навіть унеможливити виконання поставленого завдання. Низька хмарність, тумани й опади ускладнюють, а інколи виключають можливості зльоту і посадки БпЛА. Значний вплив метеорологічні умови здійснюють на можливість застосування цільової апаратури, характерної БпЛА І класу, а саме камер видимого та інфрачервоного діапазонів. Особливо великого значення набуває облік метеорологічної обстановки при масовому використанні літальних апаратів усіх типів в бойовій обстановці. Отже, погода – це один із чинників, які впливають на можливість застосування авіації, у тому числі і БпЛА.

Відповідно до вимог правил виконання польотів, що визначено наказом від 05.01.2015 року № 2 „Про затвердження Правил виконання польотів державної авіації України”, є 12 видів забезпечення польотів БпЛА. Одним з таких видів і є метеорологічне забезпечення. Виходячи з керівних документів, щодо метеорологічного забезпечення авіаційних підрозділів державної авіації Збройних Сил України, для виконання польотного завдання необхідно отримати метеоумови за бюлетнем погоди.

Підрозділи БпЛА І класу, які перебувають на озброєнні підрозділів сухопутних військ не мають своїх органів та засобів надання метеорологічного забезпечення підрозділам БпЛА. Тому досить часто у військових частинах обов'язки щодо забезпечення підрозділів БпЛА метеорологічною інформацією покладаються як додаткове навантаження на особовий склад, який не має відповідного фаху. Враховуючи той факт, що в керівництві з льотної експлуатації будь-яких БпЛА, є різні метеорологічні обмеження і для того щоб спростити задачу посадовим особам, на яких покладенні обов'язки щодо отримання такої інформації варто створити автоматизовану систему отримання метеоумов за відповідним бюлетнем, що додатково потребує розробки методики отримання даних про метеорологічні умови автоматизованим способом.

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ ПРОГНОЗУВАННЯ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ У ЗСУ

Актуальність даної теми досить висока, що пов'язане в першу чергу з інтеграцією України в Європейський Союз та запуск процесів реформування та модернізації Збройних Сил України, в основному, спираючись на тенденції розвитку країн членів НАТО. Адже ступінь автономії в системах озброєнь постійно зростає завдяки швидкому прогресу в сферах штучного інтелекту (ШІ) та робототехніки. Індустрія озброєнь також використовує можливості штучних нейронних мереж (ШНМ): зброя стає більш швидкою і ефективною, а небезпека для військових, які її використовують, зменшується за рахунок можливості безконтактного управління. Загальносвітові тенденції дозволяють зробити висновки, що тема застосування штучного інтелекту та штучних нейронних мереж є однією з найбільш перспективних та популярних сьогодні у всіх сферах, і збройні сили не є виключенням.

Мета дослідження полягає у проведенні дослідницької та аналітичної роботи щодо можливостей та реальних перспектив використання штучних нейронних мереж у процесах модернізації ЗС України за рахунок виконання наступних завдань:

- дослідження та аналіз існуючих актуальних можливостей використання досягнень ШІ та ШНМ у процесах модернізації та нарощення могутності збройних сил країн членів НАТО;

- дослідження та аналіз актуальних та реальних перспектив можливостей застосування ШІ та ШНМ у ЗС України.

Виклад основного матеріалу. Штучна нейронна мережа – математична модель, принцип роботи якої нагадує роботу мережі біологічних нейронів. Кожен шар представлений множиною вузлів – штучних нейронів, які видобувають ознаки все більшого рівня, поки останній шар не скомбінує ці ознаки, щоб зробити передбачення. Під час проведення дослідження було проаналізовано сучасний стан та тенденції розвитку технологій, методів та засобів штучного інтелекту стосовно застосування їх в оборонній сфері. Офіційна назва такої зброї звучить „автономні системи зброї летальної дії”, англійською: Lethal Autonomous Weapon Systems (скорочено LAWS). Найчастіше йдеться про бойових роботів, однак також це можуть бути дрони, безпілотні підводні човни чи автомобілі. Міжнародний комітет Червоного Хреста (МКЧХ) описує їх як зброю, яка самостійно, тобто без людського втручання, вибирає цілі та атакує їх. Повністю автономних систем зброї, які можуть чинити смертоносне насильство щодо людей, поки не існує. Однак у силу швидкого прогресу у сферах штучного інтелекту та робототехніки їхня розробка є лише питанням часу. Дослідження в області штучного інтелекту вказують на те, що їх результати доцільно використовувати при визначенні та реалізації напрямків подальшого розвитку систем управління силами і засобами збройної боротьби. Практична реалізація концепції ситуаційного управління припускає використання методів штучного інтелекту, що зумовлює необхідність комплексного застосування технологій обробки знань, нечіткої логіки та нейромережових методів для вирішення задач обробки неструктурованої інформації про стан оперативного-тактичної обстановки на полі бою.

Висновки. Отже, у ході наукового дослідження виконано аналіз загальних відомостей про досвід застосування штучних нейронних мереж у збройних силах країн членів НАТО та перспективи їх застосування у Збройних Силах України. Викладений матеріал доцільно використовувати під час визначення шляхів вдосконалення системи озброєння і військової техніки, як на середньострокову, так і довгострокову перспективу її розвитку. А також під час планування можливостей подальшого розвитку системи управління, силами та засобами збройної боротьби і її засобів (комплексів).

МЕТОДИ ТА ЗАСОБИ ФОРЕНЗИКИ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Актуальність. У міру того, як комп'ютери, комп'ютерні мережі, обчислювальні пристрої в цілому набувають широкого поширення, шанс виникнення злочинів, пов'язаних із такими пристроями, зростає. Для виявлення слідів атак в комп'ютерних мережах, зловмисників що їх здійснюють й збору доказів щодо них, необхідно мати відповідні розроблені методики й засоби проведення слідчих дій, які прийнято називати форензикою. Наразі існують роботи які розкривають методології форензики в комп'ютерних мережах, але здебільшого описують роботу слідчого з юридичної точки зору. Тому **постає задача** щодо необхідності розробки методики проведення комп'ютерно-технічної експертизи в комп'ютерних мережах і аналізу апаратно-програмних засобів для цього.

Мета. Запропонувати методику проведення та інструменти проведення криміналістичного аналізу в комп'ютерних мережах.

Основні положення. Одним із сервісів, які надають команди реагування на інциденти комп'ютерної безпеки CERT/CSIRT, є аналіз інцидентів, який полягає в оцінці всієї доступної інформації й допоміжних доказів або артефактів, що пов'язані з інцидентом або подією. Якщо зазначені інциденти мають кримінальні ознаки, то застосовується ретельний, методичний процес проведення вже криміналістичного аналізу, який характеризується чітко прописаною процедурою та правилами його проведення. Згідно стандартів WSSN (World Standards Services Network), ISO (International Organization for Standardization) експерти-криміналісти повинні бути підготовлені та кваліфіковані для майстерного поводження з цифровими доказами та повинні мати надійні технічні знання для вибору найкращих методів проведення розслідування. Адекватне та постійне навчання, а також періодичне оцінювання знань та вмінь забезпечують компетентність експертам та дають їм можливість для обробки цифрових пристроїв, які можуть містити потенційні цифрові докази (ISO / IEC 27037). Необхідний рівень компетентності експертів-криміналістів може відрізнятися від юрисдикції кожної країни. На даний момент не існує міжнародного узгодженого мінімального рівня підготовки та сертифікації. Тому для ефективного проведення розслідувань комп'ютерних злочинів було розглянуто моделі для проведення розслідувань та аналізу кіберзлочинів, що були представлені науковцями на науково-дослідних семінарах різних держав. Так, до них увійшли найбільш поширені: Digital Forensics Workshop Investigative Model (DFRWS), Abstract Digital Forensics Model (ADFM), Integrated Digital Investigation Process (IDIP), Enhanced Digital Investigation Process Model (EDIP), Computer Forensics Field Triage Process Model (CFFTPM), Digital Forensic Model based on Malaysian Investigation Process (DFMMIP).

Як результат їх аналізу й синтезу запропоновано методику проведення криміналістичного аналізу, який повинен виконати спеціаліст з комп'ютерної криміналістики, під час розслідування кримінального злочину в апаратно-програмних засобах. Вона полягає у виконанні наступних кроків: розібратись в способі реалізації злому, побудувати сценарій атаки, відновити її хронологію, зібрати решту слідів атаки, розробити необхідні заходи для запобігання подібної атаки, зменшити і відновити завдані збитки.

Для виконання цієї методики в цілому, або окремого її кроку необхідно використовувати спеціальний інструментарій, який підбирається індивідуально в залежності від поставленого завдання. До найбільш поширених можна віднести: Autopsy, Guymager, Volatility, FTKImager.

Висновок. Отже, представлена методологія та інструментарій надають можливості щодо ефективного проведення розслідувань комп'ютерних злочинів в комп'ютерних мережах та апаратно-програмних засобах.

ВИБІР РЕЖИМУ РОБОТИ ВІЙСЬКОВИХ ЗАСОБІВ РАДІОЗВ'ЯЗКУ В УМОВАХ СКЛАДНОЇ РАДІОЕЛЕКТРОННОЇ ОБСТАНОВКИ

На якість військового радіозв'язку впливають завмирання сигналів, які виникають внаслідок багатопроменевого розповсюдження радіохвиль, та навмисні завади, що створюються системою радіоелектронного подавлення (РЕП) супротивника. Крім того, суттєвою перешкодою для оптимального приймання сигналів є апіорна невизначеність характеристик каналу зв'язку. Завдання забезпечення стійкого радіозв'язку в умовах складної радіоелектронної обстановки, яка постійно змінюється, можливо за рахунок вибору режиму роботи військових засобів радіозв'язку (ЗРЗ), що забезпечує задані вимоги до якості передачі інформації. Одним з шляхів підвищення ефективності функціонування ЗРЗ є використання широкосмугових сигналів (ШСС). Широкосмугові сигнали, на відміну від вузькосмугових, мають вищу завадо- і протирозвідувальну захищеність.

Широке застосування у телекомунікаційних системах, перш за все, спеціального призначення, знаходять ШСС, одержувані методом прямої послідовності (DSSS – Direct SSS). У таких системах розширення спектра здійснюється шляхом множення порівняно вузькосмугового первинного сигналу на широкосмуговий розширювальний сигнал.

Серед методів формування ШСС широке практичне застосування одержав метод псевдовипадкового перестроювання робочої частоти (ППРЧ), при якому розширення спектра в межах заданої смуги частот здійснюється за допомогою стрибкоподібної зміни частоти сигналу за псевдовипадковим законом, невідомим постановнику завад.

В сучасних системах радіозв'язку широко використовується один із методів формування широкосмугових сигналів – метод ортогонального частотного розділення з мультиплексуванням (Orthogonal Frequency Division Multiplexing – OFDM). Основними перевагами даного методу є відносно висока стійкість щодо частотно-селективних завмирань і вузькосмугових завад, а також висока спектральна ефективність. Але при наявності в каналі навмисних завад, особливо імітаційно-дезінформуючих, ефективність функціонування засобів радіозв'язку з OFDM значно знижується, іноді до повної втрати переданої інформації.

Дослідження показали, що для різних сценаріїв радіоелектронної обстановки ефективними виявляються певні режими роботи ЗРЗ.

Так для каналу зв'язку з селективними завмираннями та вузько смуговими завадами ефективним є режим OFDM. Для випадку дії в каналі імітаційних завад доцільним є розширення OFDM-сигналу псевдовипадковими послідовностями (ПВП) дозволяє значно зменшити вплив навмисних завад. По-перше, зменшення впливу завад забезпечується ефектом „розмивання” завад по спектру за рахунок перемноження прийнятої суміші сигналу і завади з ПВП. По-друге, завадостійкість приймання OFDM-сигналу значно підвищується за рахунок підвищення стійкості пілот-сигналів (пілот-несучих) щодо впливу завад, що забезпечує більш точну оцінку поточного стану каналу зв'язку. Знання передаточної характеристики каналу, в свою чергу, дозволяє застосувати режекцію частини спектра, ураженої завадою, з відключенням передачі корисної інформації по відповідних піднесучих. По-третє, якщо противник застосовує імітаційну заваду, яка в точності відтворює структуру сигналу, теоретично він не знає способу генерації ПВП. Тому така імітаційна завада хоч і буде створювати ефект внутрішньосистемних завад внаслідок неортогональності ПВП, що генеруються постановником завад і ЗРЗ, однак ефективність її значно зменшиться внаслідок узгодженої фільтрації після перемноження в кореляторі приймача.

Для ретрансльованих завад ефективним є режим ППРЧ. При цьому за рахунок вибору швидкості перестроювання частоти необхідно забезпечити можливість повністю позбавитись від їхнього впливу.

Результати імітаційного моделювання показують, що застосування адаптивної зміни режимів роботи у військових системах радіозв'язку дозволяє значно підвищити ефективність їх функціонування в умовах активного радіоелектронного подавлення.

КОМПЛЕКСНА МЕТОДИКА УПРАВЛІННЯ ПАРАМЕТРАМИ ВІЙСЬКОВИХ РАДІОМЕРЕЖ В УМОВАХ НЕВИЗНАЧЕНОСТІ РАДІОЕЛЕКТРОННОЇ ОБСТАНОВКИ

Проведення Антитерористичної операції на території Донецької та Луганської областей (Операції об'єднаних сил) показало недосконалість існуючої системи управління і зв'язку, основу якої складають засоби радіозв'язку (ЗРЗ). Основними недоліками існуючої системи зв'язку тактичної ланки управління Збройних Сил України є: низька мобільність вузлів зв'язку пунктів управління; низька продуктивність, надійність, розвід та завадозахищеність; низька автоматизація процесів встановлення, ведення та підтримання радіозв'язку.

Основними технічними вимогами для наступного покоління систем зв'язку є: інтеграція всіх видів трафіку (мова, дані, відео, відеоконференція); повна мобільність всіх абонентів і елементів системи; забезпечення заданої якості обслуговування користувачів; гарантоване засекречування усіх видів інформації.

Проведений аналіз можливих варіантів побудови архітектури мереж тактичної ланки управління провідних держав світу продемонстрував переваги застосування мобільних радіомереж або MANET (Mobile Ad-hoc Networks) в порівнянні з іншими підходами. Класичний централізований підхід до управління каналними та мережевими ресурсами систем військового радіозв'язку не відповідає вимогам сучасності, тому авторами даного дослідження запропоновано в якості базового принципу побудови тактичних мереж зв'язку використати принцип функціонування мобільних радіомереж з можливістю самоорганізації.

У ході дослідження запропоновано комплексну методику управління параметрами військових радіомереж в умовах невизначеності радіоелектронної обстановки, сутність якої полягає в забезпеченні підтримки заданих значень показників функціонування систем військового радіозв'язку на належному рівні.

За основу взято принцип управління, що описаний в еталонній мережевій моделі взаємодії відкритих систем, проте з деякими доповненнями та змінами. Зазначений підхід в цілому дозволяє здійснювати наскрізне управління каналними та мережевими ресурсами систем військового радіозв'язку в складній радіоелектронній обстановці.

Методика складається з наступної послідовності дій:

1. Введення вихідних даних та оцінка радіоелектронної обстановки в мережі в цілому та для кожного окремого радіонапряму;
2. Прогнозування стану радіоелектронної обстановки системи радіозв'язку та для окремого радіонапряму мережі;
3. Вибір робочих частот з урахуванням стратегії засобів радіоелектронного подавлення;
4. Формування топології системи радіозв'язку;
5. Управління маршрутизацією;
6. Вибір режиму роботи.

Запропоновану в роботі комплексну методику доцільно використовувати при розробці програмного забезпечення для модулів (блоків) оцінки перспективних засобів радіозв'язку, що засновано на інтерфейсах відкритої архітектури версії SCA 2.2, що дозволить: використовувати ефективні сигнально-кодові конструкції для забезпечення завадозахищеності каналів; забезпечити ефективне використання радіочастотного ресурсу програмованих засобів радіозв'язку; підвищити швидкість оцінки каналів зв'язку; зменшити використання обчислювальних ресурсів засобів радіозв'язку з програмованою архітектурою.

Оцінка ефективності запропонованої методики показала підвищення завадозахищеності засобів радіозв'язку до 30 % при її використанні.

АНАЛІЗ ЗАСТОСУВАННЯ МЕТОДУ ГЛИБОКОГО ВИВЧЕННЯ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ ТА ШВИДКОГО РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

Актуальність. Швидкий розвиток інформаційних технологій та зростання обсягів інформації, яка обробляється, зберігається та передається в кіберпросторі набуває глобального характеру. Державні кордони та відстані вже не є суттєвою перешкодою для руху інформаційних потоків, також суттєво зросло і продовжує зростати значення доступу до інформації для розвитку різних сфер людської діяльності. Все це призвело до збільшення кількості кіберінцидентів, які призводять до зриву, блокування роботи системи, або несанкціонованого управління її ресурсами, ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

З кожним днем кількість кіберінцидентів зростає, з'являються нові раніше невідомі реалізації кібератак.

Ефективність функціонування сучасних систем та технологій виявлення кіберзагроз істотно залежить від оперативності їх виявленні.

Для забезпечення виявлення кіберзагроз застосовуються статистичні, сигнатурні методи та методи виявлення аномалій. Так, найточніший на сьогодні метод, що ґрунтується на сигнатурному аналізі, добре функціонує при виявленні вже відомих вторгнень, але абсолютно не придатний для виявлення нових, раніше невідомих. Метод виявлення аномалій такого недоліку немає та є ефективним при появі нових або модифікованих видів кіберзагроз.

Для виявлення аномалій широко використовується метод машинного навчання.

Метою роботи є аналіз застосування методу глибокого вивчення штучних нейронних мереж для виявлення кіберзагроз та швидкого реагування на кіберінциденти.

Основна частина. Машинне навчання – це метод аналізу даних, який автоматизує побудову аналітичної моделі. Це галузь штучного інтелекту, заснована на ідеї, що системи можуть вчитися на основі даних, визначати закономірності та приймати рішення з мінімальним втручанням людини.

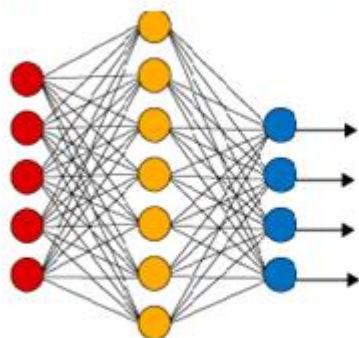
Для машинного навчання використовують різні технології та алгоритми. Зокрема, можуть застосовуватися дискримінантний аналіз, байєсовські класифікатори та багато інших математичних методів. Але в кінці ХХ століття все більше уваги почали приділяти штучним нейронним мережам (ШНМ). Штучні нейронні мережі є системою з'єднаних і взаємодіючих між собою штучних нейронів, виконаних на основі порівняно простих процесорів. Кожен процесор ШНМ періодично отримує сигнали від одних процесорів (або від сенсорів, або від інших джерел сигналів) і періодично посилає сигнали іншим процесорам. Всі разом ці прості процесори, з'єднані в мережу, здатні вирішувати досить складні завдання.

Найчастіше нейрони розташовуються в мережі за рівнями (їх ще називають шарами). Нейрони першого рівня – це, як правило, вхідні. Вони отримують дані ззовні (наприклад, від сенсорів системи розпізнавання осіб) і після їх обробки передають імпульси через синапси нейронів на наступний рівень. Нейрони на другому рівні (його називають прихованим, оскільки він безпосередньо не пов'язаний ні з входом, ні з виходом ШНМ) обробляють отримані імпульси і передають їх нейронам на вихідному рівні. Оскільки мова йде про імітацію нейронів, то кожен процесор вхідного рівня пов'язаний з декількома процесорами прихованого рівня, кожен з яких, в свою чергу, пов'язаний з декількома процесорами рівня вихідного. Така архітектура найпростішої ШНМ, яка здатна до навчання і може знаходити простий взаємозв'язок в даних. На сьогоднішній день широко використовується поняття глибокого навчання ШНМ.

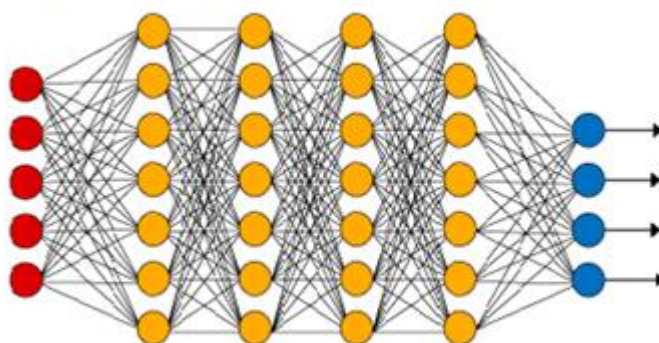
Глибоке навчання ШНМ – це клас алгоритмів машинного навчання у вигляді нейронної мережі, що використовує каскад шарів, блоків обробки для отримання функцій з даних і прогнозування нових даних.

Глибоке (глибинне) навчання ШНМ може бути застосоване лише по відношенню до більш складних ШНМ, що містить кілька прихованих рівнів. При цьому рівні нейронів можуть чергуватися з шарами, які виконують складні логічні перетворення. Кожен наступний рівень мережі шукає взаємозв'язки в попередньому. Така ШНМ здатна знаходити не тільки прості взаємозв'язки, а й взаємозв'язки між взаємозв'язками. На рис. 1 представлено просту нейронну мережу та нейронну мережу глибокого навчання.

Проста нейронна мережа



Нейронна мережа глибокого навчання



● Вхідний рівень ● Прихований рівень ● Вихідний рівень

Рис. 1 Структура нейронних мереж

В галузі кібербезпеки глибоке навчання ШНМ допомагає змінити спосіб вирішення питань безпеки. Нейронні моделі глибокого навчання ШНМ можуть передбачати та захищати організації від відомих та невідомих кібератак у режимі реального часу, одночасно пом'якшуючи проблему помилкових спрацьовувань. Глибоке навчання ШНМ працює як людський мозок, пропонуючи високі показники точності. Великою силою глибокого навчання ШНМ для кібербезпеки є те, що воно дає змогу вчитися в режимі реального часу та розробляти нові критерії класифікації без участі людини. Завдяки цьому виявлення кібератак та класифікація стають кібератак набагато ефективнішими та активнішими.

На сьогоднішній час багато розробників засобів захисту інформації та забезпечення кібербезпеки заявляють, що вони використовують методи машинного навчання у своїй продукції. До основних засобів, які використовують методи МН на основі ШНМ відносяться: системи антивірусного захисту, системи виявлення та запобігання вторгненням (IDS/IPS), системи попередження втрати даних (DLP), системи управління інформаційною безпекою та подіями (SIEM), системи розслідування порушень кібербезпеки та інші.

Висновки: Постійне зростання кіберзлочинності залишається проблемою з точки зору практики безпеки та конфіденційності. За допомогою методу глибокого навчання ШНМ в галузі кібербезпеки досягли значного прогресу в системах виявлення вторгнень, в аналізі шкідливого коду, мережевого трафіку, поведінки користувачів, виявленні спаму та соціальній інженерії.

Метод глибокого навчання ШНМ при подальшому використанні в галузі кібербезпеки зможе забезпечити покращення роботи різних систем для виявлення кібератак, їх моделювання, моніторингу та аналізу, а також захист від різних загроз для конфіденційних даних та систем безпеки, а також забезпечить швидке реагування на кіберінциденти.

ТРОПОСФЕРНІ СТАНЦІЇ НОВОГО ПОКОЛІННЯ НА ОСНОВІ SDR-ТЕХНОЛОГІЇ

Незважаючи на те, що тропосферно радіорелейні станції (ТРРС) значно складніші в реалізації, а пропускна здатність їх нижча, ніж у радіорелейних станціях (РРС) прямої видимості, завдяки більшій довжині прольотів ТРРС набули досить широкого застосування, особливо у військовій сфері.

Розгортання тропосферних станцій не висуває складних вимог до рельєфу місцевості. Не потрібно установки високих щогл, необхідних у випадку РРЛ для забезпечення прямої видимості.

Основними особливостями тропосферного поширення радіохвиль, є дуже велике загасання радіосигналу на ділянці поширення й завмирання сигналу на вході приймача, які мають селективний за частотою характер.

У випадку традиційного підходу для забезпечення стійкого зв'язку доводиться підвищувати енергетичні параметри обладнання ТРРС через збільшення потужності випромінювання передавачів, використання малошумливих підсилювачів на вході приймачів та застосування антен більших розмірів.

Усе це призводить до значного збільшення габаритних розмірів ТРРС.

До недоліків традиційних засобів загоризонтного радіорелейного зв'язку також належать: низька надійність зв'язку в умовах завад, відсутність автоматизованих антенно-щоглових пристроїв, низькі характеристики з електромагнітної сумісності.

Одним з основних недоліків традиційних ТРРС при збереженні необхідної завадостійкості в умовах багатопромених завмирань є створення ефективних портативних ТРРС нового покоління.

Станція повинна мати можливість працювати в трьох режимах: тропосферного, прямої видимості та дифракційного поширення. При цьому забезпечується висока вірогідність передачі інформації (у тропосферному режимі $BER = 10^{-5}$, у режимі прямої видимості $BER = 10^{-6}$) за високого коефіцієнта готовності радіолінії (0,98).

Складні умови зв'язку при тропосферному поширенні вимагають використання багаторівневої адаптації: часової в межах смуги робочих частот (адаптивна модуляція і кодування); частотної, яка передбачає вибір оптимальної робочої частоти й оптимальної смуги робочих частот; просторової, яка передбачає використання багатоантенної техніки і технології MIMO (Multiple Input – Multiple Output); міжрівневої, що передбачає оптимальне використання адаптивної модуляції та кодування і технології гібридного автоматичного запиту на повторну передачу даних HARQ (Hybrid Automatic Repeat Request).

Реалізація портативних ТРРС нового покоління потребує відповідного високоефективного спеціалізованого каналоутворюючого обладнання, основою якого є програмований модемний пристрій на основі технології SDR (Software Defined Radio).

Він дає змогу застосувати більш ефективні методи формування та обробки сигналів при прийомі з метою зменшення відношення сигнал/шум на вході приймача, за якого забезпечуються виконання норм на якісні показники каналів і досить висока пропускна здатність.

ІМІТАЦІЙНА МОДЕЛЬ БАГАТО ПРОЦЕСОРНОЇ ОБИСЛЮВАЛЬНОЇ СИСТЕМИ ЗІ СПІЛЬНОЮ ПАМ'ЯТТЮ

Актуальність дослідження обумовлена необхідністю вдосконалення можливостей апаратної структури управління військами при інтеграції новітніх систем управління військами Збройних Сил України і, як слідство, у підвищенні ефективності виконання задач які ставляться перед бойовими підрозділами .

Витрати часу та складність прийняття рішень збільшується при переході від нижчого рівня до верхнього, а з використанням багатопроцесорних систем час на прийняття рішення для кожної конкретної задачі, навпаки, зменшується. Звідси випливає, що заміна апаратних частин телекомунікаційних вузлів та пунктів управління починаючи від батальйона та вище суттєво підвищить бойові можливості бойових підрозділів при значному навантаженні при інтенсивних бойових діях, що визначає ефективність функціонування системи управління в цілому.

Мета дослідження полягає у підвищенні ефективності процесів управління військами, планування бойового застосування частин за рахунок виконання **наступних часткових завдань дослідження**:

- аналіз сучасного підходу у плануванні вузлів зв'язку на пунктах управління системи зв'язку у Збройних Силах України, спираючись на вимоги керівних документів з організації зв'язку;
- вдосконалення планування багатопроцесорних систем за рахунок використання кластерів та процесів, що пов'язані з цією задачею, з урахуванням недоліків та обмежень сучасної моделі;
- автоматизація процесів відправлення та прийняття даних за рахунок використання технології паралельної обробки . Апробація моделей.

Виклад основного матеріалу. Однією з відмінних рис багатопроцесорної обчислювальної системи є мережа обміну, за допомогою якої процесори з'єднуються один з одним або з пам'яттю. Модель обміну настільки важлива для багатопроцесорної системи, що багато характеристик продуктивності та інші оцінки виражаються відношенням часу обробки до часу обміну, відповідним важливість справ. Існують дві основні моделі між процесорного обміну: одна заснована на передачі повідомлень, інша - на використанні загальної пам'яті. У багатопроцесорній системі із загальною пам'яттю один процесор здійснює запис в конкретний осередок, а інший процесор виробляє зчитування з цього осередку пам'яті. Щоб забезпечити узгодженість даних і синхронізацію процесів, обмін часто реалізується за принципом взаємно виключного доступу до спільної пам'яті методом „поштової скриньки ”. В архітектурі з локальною пам'яттю безпосереднє розділення пам'яті неможливо. Замість цього процесори отримують доступ до спільно використовуваних даних за допомогою передачі повідомлень по мережі обміну. Ефективність схеми комунікацій залежить від протоколів обміну, основних мереж обміну і пропускної здатності пам'яті і каналів обміну

Висновки. Отже, в роботі запропоновано використання багатопроцесорної обчислювальної системи зі спільною пам'яттю для заміни апаратної частини вузлів зв'язку на пунктах управління для підвищення ефективності виконання завдань бойовими підрозділами.

РОЗРАХУНКИ МАКСИМАЛЬНОЇ ДАЛЬНОСТІ ЗВ'ЯЗКУ У РАДІОМЕРЕЖАХ З ПОВІТРЯНИМИ РЕТРАНСЛЯТОРАМИ НА БПЛА

В останні роки все більшого поширення набуває ідея застосування ретрансляторів УКХ радіомереж на борту малогабаритних безпілотних літальних апаратів (БПЛА). Це дозволяє отримати низку переваг, основними з яких є збільшення дальності зв'язку у радіомережі, розширення зони покриття повітряного ретранслятора, порівняно з наземним, усунення мертвих зон, підвищення зв'язності радіостанцій у мережі.

Очевидно, що важливим завданням є визначення координат (траєкторії баражування) БПЛА. Враховуючи можливий вплив засобів радіоелектронної боротьби (РЕБ) противника, а також значну висоту підйому, необхідно забезпечити достатнє віддалення ретранслятора від засобів РЕБ, а отже – і від радіостанцій власної мережі. Тому БПЛА з повітряним ретранслятором повинен рухатися у тилу підрозділів, в інтересах яких він забезпечує зв'язок. У той же час, віддалення БПЛА призводить до зменшення рівнів сигналу на входах приймачів. Тому важливим та актуальним завданням є визначення граничної дальності зв'язку при забезпеченні необхідної швидкості передачі інформації із заданою якістю.

Сучасні засоби УКХ радіозв'язку та засоби широкосмугового безпроводового доступу (ШБД) підтримують декілька режимів роботи, які можуть відрізнятися шириною смуги каналу, видом модуляції, схемою завадостійкого кодування, потужністю передавача, чутливістю приймача та іншими параметрами. В залежності від необхідної швидкості передачі та, відповідно, інших параметрів радіолінії, дальність зв'язку може коливатися у широких межах. Основним чинником, який визначає дальність зв'язку в діапазоні УКХ, є рельєф місцевості та місцеві предмети (будівлі, насадження тощо).

Очевидно, що завдання визначення дальності зв'язку на практиці розв'язати можна, як правило, тільки наближено. Проте навіть приблизний розрахунок є доцільним на етапі планування радіомереж з повітряними ретрансляторами.

Для визначення можливості забезпечення зв'язку між кореспондентами із заданими координатами необхідно розв'язати задачу з розрахунку рівня сигналу на вході приймача, що представляє собою рівняння радіолінії. Максимально можлива (гранична) дальність зв'язку (із забезпеченням заданих вимог щодо якості передачі інформації) буде досягатися при наближенні сигналу на вході приймача до величини його реальної чутливості. Тому визначити граничну дальність зв'язку можна, якщо виразити відстань у складовій втрат у вільному просторі через інші складові рівняння радіолінії. При цьому, замість значення очікуваного рівня сигналу в точці прийому необхідно підставити значення чутливості приймача.

Для більш точної оцінки дальності зв'язку між БПЛА та наземними радіостанціями в реальних умовах можна скористатися відомою моделлю Хата для умов міста та відкритої (сільської) місцевості. Модель Хата можна застосовувати при виконанні наступних умов: діапазон частот 100 – 1500 МГц, відстань 1 – 300 км, висота антени базової станції h_1 від 30 до 200 м, висота антени мобільної станції – 1 – 10 м.

Отримані результати розрахунків граничної дальності зв'язку для УКХ радіостанцій та засобів ШБД можуть використовуватись при плануванні зв'язку між БПЛА або БПЛА та іншими повітряними об'єктами (при забезпеченні між ними відкритого інтервалу), а також для орієнтовної оцінки граничної дальності зв'язку наземних радіостанцій з повітряним ретранслятором.

При плануванні траєкторії руху БПЛА необхідно враховувати не тільки показники орієнтовної (граничної) дальності зв'язку, а і забезпечення максимальної завадозахищеності.

АКТУАЛЬНІСТЬ ОНОВЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ РАДІОСТАНЦІЙ L3HARRIS

Радіостанції L3Harris являються програмно реалізованими засобами зв'язку. Виробник постійно вдосконалює програмне забезпечення обладнання, що розширює його можливості.

В нових версіях програмного забезпечення зазвичай покращуються наявні форми сигналів, а в деяких випадках з'являються абсолютно нові функції.

Обладнання L3Harris постачається в Збройні Сили України та інші силові структури держави протягом декількох років.

Це створює ситуацію, коли однотипні радіостанції різних років постачання мають різні версії програмного забезпечення і не можуть забезпечити 100% сумісну роботу в мережах зв'язку.

Разом з мікропрограмами обладнання відповідно оновлюються і можливості застосунку для створення файлів конфігурацій та програмування радіостанцій Communication Planning Application.

Всі оновлення програмного забезпечення від L3Harris супроводжуються актуальними посібниками з експлуатації та іншими довідковими матеріалами.

Яскравими прикладами вдосконалення можливостей обладнання за рахунок оновлення програмного забезпечення є мікропрограма версії 4.7.0 для сімейства радіостанцій RF-7850M, RF-7800V та мікропрограма версії 2.1 для сімейства радіостанцій RF-7800H.

В першому випадку радіостанції VHF та UHF діапазонів отримують підтримку форми сигналів TNW-75, що використовує ППРЧ з доступом до каналу TDMA і шириною смуги каналу 25 кГц або 75 кГц та забезпечує передачу голосу, даних, звітів ситуативної обізнаності.

Радіостанції сімейства RF-7850M додатково отримують підтримку адаптивної мережевої широкосмугової форми сигналів ANW2C, що використовує ширину смуги каналу 1,2 МГц, забезпечує роботу до 30 користувачів в мережі та дозволяє розширити розгорнуту локальну тактичну IP мережу.

В другому випадку радіостанції сімейства RF-7800H отримали підтримку форми сигналу VULOS, що забезпечує зв'язок на фіксованій частоті в межах прямої видимості в діапазоні частот VHF, та режиму роботи 3GIP, який дозволяє проводити обмін IP даними з використанням як широкосмугових, так і вузькосмугових каналів.

Мікропрограма версії 2.1 містить істотно покращений протокол KX зв'язку третього покоління (3G), що підтримує роботу до 124 радіостанцій.

Крім цього, повністю оновлено інтерфейс користувача, змінено процедуру програмування радіостанції та забезпечено можливість збереження в пам'яті пристрою декількох планів місії з функцією їх активації за необхідності.

Радіостанції L3Harris за рахунок програмної реалізації та постійного вдосконалення програмного забезпечення обладнання мають досить гнучку функціональність.

Для коректної сумісної роботи та максимального використання можливостей пристроїв рекомендовано проводити планове оновлення програмного забезпечення в підрозділах.

БАГАТОКАНАЛЬНА УНІВЕРСАЛЬНА РАДІОСТАНЦІЯ L3HARRIS RF-7850D

Вкрай важливим для будь-якого завдання є повноцінний зв'язок з усіма взаємодіючими підрозділами. Це викликає необхідність в засобах зв'язку, які могли б об'єднати в одну мережу радіостанції різного призначення з відмінними технічними характеристиками. При цьому подібне обладнання має бути малогабаритним, спроможним підтримувати роботу з існуючими формами сигналів і мати можливість інтегруватись в мережі з формами сигналів наступного покоління.

Радіостанція L3Harris RF-7850D є ідеальним малогабаритним багатоканальним засобом зв'язку для бойових машин та командних пунктів. Ця універсальна радіостанція надає користувачу можливість використовувати два канали в діапазоні частот 30-512 МГц одночасно або додатковий другий канал в суцільному діапазоні частот 30-2500 МГц. При використанні в автомобільному варіанті RF-7850D легко встановлюється в низькопрофільне шасі і не заважає водію та екіпажу. RF-7850D – це радіостанція, що забезпечує безперебійний зв'язок та взаємодію усіх ланок на полі бою, від окремого бійця до пунктів управління та повітряних платформ в VHF та UHF діапазонах. RF-7850D реалізована на базі архітектури SDR (Software-defined radio) для радіостанцій наступного покоління VOE (Versatile Operating Environment), що забезпечує сумісну роботу з системами попередніх поколінь Falcon I та Falcon II, та може використовувати переваги нових режимів роботи, форм сигналів та мережевих технологій. VOE забезпечує підтримку найкращих в своєму класі вузькосмугових (TNW25, TNW75), широкосмугових (M-TNW, ANW2C, S-TNW, V-TNW), стійких до радіоподавлення (Quicklook 3, Quicklook Wide) форм сигналів та форм сигналів взаємодії (HAVEQUICK I/II, SATURN). Доступ до провідних системних рішень забезпечується за допомогою звичайних інтерфейсів USB, Ethernet, WPAN та GPS. Підтримка бездротової персональної мережі (WPAN) включає точку доступу Wi-Fi, Bluetooth, BLE (Bluetooth Low-Energy). При роботі з підсилювачем L3Harris RF-410 вихідна потужність системи RF-7850D-VS зростає до 50 Вт в діапазоні частот 30-2500 МГц і розширює можливості режимів роботи та управління для всієї бібліотеки сигналів. RF-7850D-VS також включає інтерфейс функціонального модуля L3Harris, за допомогою якого розширюються можливості радіостанції, починаючи від нових форм сигналів і закінчуючи комерційними рішеннями.

Функціональний модуль забезпечує наявність повноцінного третього каналу. Радіостанція може використовуватись для одночасної роботи в трьох різних мережах, як в єдиній загальній мережі. Комплект RF-7850D включає повний пакет застосунків для тактичних потреб (hC2, hManager, та ін.), розроблений для роботи на різних пристроях та веб-браузерах.

Радіостанція підтримує взаємодіючий алгоритм шифрування AES 128-bit і 256-bit, запатентований алгоритм Citadel II та модифікацію алгоритму клієнта (CAM) для унікальних криптографічних можливостей.

Радіостанція L3Harris RF-7850D за рахунок її модульності є універсальним рішенням для багаторівневих мереж. Завдяки тому що RF-7850D в 3 рази компактніша за інші подібні радіостанції, відчутно збільшується варіативність її встановлення, що забезпечує економію місця для решти критично необхідного обладнання. RF-7850D - це перша радіостанція, яка легко поєднує роботу обладнання різних поколінь і забезпечує інтеграцію новітніх радіостанцій в наявні мережі.

ПРИНЦИПИ ПОБУДОВИ КОГНІТИВНИХ РАДІОМЕРЕЖ

Сучасні безпроводові мережі характеризуються статичним розподілом спектру, згідно з яким певні смуги спектру на довгостроковій основі призначаються для використання тим чи іншим мережам (постачальникам послуг) у достатньо великих географічних регіонах. Одночасне використання в одному діапазоні частот декількох передавачів може призвести до значних взаємних завад та спотворення інформації, яка передається у різних мережах. Це значно ускладнює роботу телекомунікаційних радіосистем різного призначення. Одним із можливих шляхів розв'язання цієї проблеми є впровадження технології когнітивних радіомереж, що і визначає актуальність даної теми.

Когнітивна радіомережа передбачає механізми управління засобами різного рівня адаптації до стану радіоканалу.

Загальними властивостями когнітивних радіомереж є:

- можливість отримання інформації про стан радіосередовища (в першу чергу, завантаженість радіочастотного спектра, виділеного для роботи радіомережі);
- здатність виконувати інтелектуальний аналіз інформації про стан радіосередовища;
- здатність в адаптивному режимі змінювати параметри засобів радіозв'язку при виникненні нових умов в радіоканалі.

Когнітивні радіомережі породжують унікальні завдання, які виникають внаслідок їх співіснування з первинними мережами, що призводить до створення відповідних вимог до якості обслуговування (QoS). Отже, виникають нові функції управління радіочастотним спектром, які необхідні для когнітивних радіомереж.

Функції процесу управління радіочастотним спектром складаються з чотирьох основних етапів:

- сканування радіочастотного спектру;
- ☐ вибір смуг спектру;
- ☐ використання спільних ділянок спектру;
- ☐ мобільність радіочастотного спектру.

Основною ідеєю когнітивних радіомереж є можливість забезпечення високої пропускної здатності для мобільних користувачів за допомогою динамічних методів доступу до спектру і гетерогенної безпроводової архітектури самої мережі. Користувач такої мережі може виділити кращий із частотних каналів, при цьому вибір буде залежати не тільки від наявності вільної ділянки спектру, а визначатися на основі певних внутрішніх правил, наприклад, вимог щодо якості обслуговування (QoS) або статистичних параметрів каналу.

Управління спектром частот в стандарті *IEEE 802.22* – це когнітивна функція на базовій станції, яка використовує вхідні дані шляхом сканування частотного спектру, геолокації та діючої бази даних з метою прийняття рішення про частотний канал, що буде використовуватися. При цьому, встановлюються обмеження на потужність випромінювання для конкретного абонентського пристрою. Така реалізація базується на властивості досліджуваних систем виявляти тимчасово зайняті/незайняті ділянки спектра та переключатися між ними. Зондування спектру може застосовуватися у випадках, коли рівень виявленого сигналу достатньо великий чи завчасно відомі тип або форма сигналу.

Напрямок подальших досліджень є розробка рекомендацій щодо реалізації та впровадження когнітивних принципів у системи військового радіозв'язку, які крім взаємних завад, підлягають впливу засобів радіоелектронного подавлення противника, для чого необхідно розробити чіткі вимоги до їх технічних та експлуатаційних параметрів, геолокаційної бази даних і чітко визначити норми та правила користування частотним спектром.

СУЧАСНИЙ СТАН ТА ШЛЯХИ РОЗВИТКУ БЕЗПІЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ КЛАСУ І ДЛЯ ВИКОНАННЯ БОЙОВИХ ЗАВДАНЬ

В умовах сучасних бойових дій, актуальним залишається використання безпілотних літальних апаратів (БпЛА), що вимагає подальшого їх розвитку. З цією метою пропонується розглянути перспективи впровадження штучного інтелекту в БпЛА для виконання завдань розвідки.

БпЛА можна віднести до автономних роботизованих систем розвідки, що в умовах сучасної війни, під час виконання бойового завдання на сході України підпадають під дію засобів радіоелектронної боротьби (РЕБ), і тому втручання оператора у його роботу здебільшого є неможливим. З метою забезпечення виконання поставленого завдання розробники безпілотних авіаційних комплексів почали використовувати у них штучний інтелект з метою автоматизації усіх процесів протікаючи на борту повітряного судна, що дозволяє виконати поставлене завдання з розвідки без зв'язку з наземною станцією керування.

Історично так склалося, що безпілотні повітряні судна почали розроблятися ще в 60-х роках минулого століття. Нині 40 держав світу вже використовують понад 80 типів подібних апаратів. З початком війни на сході України в 2014 році наші збройні сили почали використовувати БпЛА різних виробників, такі як: PD-1, Лелека-100, А1-СМ „Фурія”, МП-1 «Spectator», Sparrow, RQ-11B «Raven» та багато інших, при цьому активно почалися розробка щодо їх керування із використанням технологій штучного інтелекту.

Система керування відповідає за правильність функціонування усіх систем літального апарату. До цієї системи належать система живлення, система сенсорів, датчиків та камер, система зв'язку, система стабілізації, авіоніка та інші. Під час виконання бойового завдання ця система, за допомогою штучного інтелекту, виконує роль оператора. Зазвичай вона є найбільш розвиненою.

До основних напрямків використання штучного інтелекту в БпЛА для її ефективного керування, також можна віднести й інерціальну систему позиціонування. Дана система використовується коли повітряне судно зазнало впливу засобів РЕБ і літальний апарат не має можливості отримувати свої координати GPS та команди керування від оператора, тому перспективним є втілення такого штучного інтелекту, який за допомогою датчиків лінійного прискорення (акселерометрів), гіроскопічних приладів, що відтворюють на об'єкті систему відліку (наприклад, за допомогою гіростабілізованої платформи) дозволить визначати кути повороту і нахилу об'єкта, які використовуються для його стабілізації та управління рухом. При цьому така система надасть можливість більш точно проводити обчислення та прогнозування необхідної швидкості руху БпЛА, його координат й інших параметрів руху. Дана система з використанням штучного інтелекту дозволить перевіряти курс літального апарату, і при відхиленні – формувати сигнали (команди) корегування маршруту руху БпЛА з метою його повернення на злітно-посадковий майданчик, тим самим це дозволить підвищити живучість БпЛА та забезпечить виконання поставленого бойового завдання.

Додатково на сучасному етапі розвитку інформаційних технологій широкого застосування набувають методи пошук та удосконалення методів автоматичного дешифрування об'єктів на аерознімках, отриманих з БпЛА, які б забезпечували достатню точність виявлення та розпізнавання об'єктів в складних топографічних умовах місцевості, де також найперспективнішим є використання технологій штучного інтелекту.

Таким чином, використання штучного інтелекту в безпілотних авіаційних комплексах класу І дозволить автоматизувати систему керування будь-якого БпЛА, завдяки чому можна буде більш ефективно виконувати розвідувальні завдання без втручання оператора-пілота.

ФОРМУВАННЯ НАБОРУ АПРІОРНИХ ДАНИХ НЕЙРОМЕРЕЖІ ГЕНЕРАТИВНОЮ ЗМАГАЛЬНОЮ МЕРЕЖЕЮ ДЛЯ АВТОМАТИЗОВАНОЇ ОБРОБКИ АЕРОЗНІМКІВ

В умовах невеликої кількості апріорних зображень об'єктів навчальної вибірки нейромереж, отриманих з використанням безпілотного авіаційного комплексу, незбалансованості їх класів, невідповідності умовам проведення аерозйомки, виникають обмеження, які унеможливають використання технології нейромереж для автоматизованої обробки цифрових аерознімків. Тому актуальним залишається питання розроблення підходу щодо формування необхідного набору апріорних зображень об'єктів, отриманих шляхом аерозйомки, який відрізняється адаптацією до умов зйомки та специфіки зображень об'єктів дешифрування на аерознімках.

Для завдань тематичної обробки слід використовувати підхід генеративних змагальних мереж (англ. GAN), що успішно зменшують вплив спотворень та відповідають перевагам фотореалістичного стилю в різних сценаріях, включаючи передачу часу доби, метеорологічних умов, пори року при збільшенні набору зображень об'єктів.

В основі GAN лежить теоретико-ігрова ситуація, коли диференційована генеративна мережа, що безпосередньо створює навчальні приклади $x = g(z; \theta^{(g)})$ повинна змагатися з дискримінаторною мережею, яка намагається відрізнити приклади, взяті з навчальних даних, від прикладів, створених генератором. Дискримінатор видає значення, повернене функцією $d(x; \theta^{(d)})$, що дорівнює ймовірності того, що x – реальний навчальний приклад, а не підроблений зразок, отриманий з моделі. Етапи повторюються кілька разів, в результаті чого генератор та дискримінатор стають кращими у відповідних результатах після кожного повторення.

Процес навчання в генеративній змагальній мережі описується як гра з нульовою сумою, в якій функція $v(\theta^{(g)}, \theta^{(d)})$ визначає винагороду дискримінатора. Генератор отримує $v(\theta^{(g)}, \theta^{(d)})$ в якості своєї винагороди. У процесі навчання кожен гравець прагне максимізувати свою винагороду

$$g^* = \arg \min_G \max_D V(G, D)$$

За замовчуванням V вибирається в такий спосіб:

$$\min_G \max_D V(G, D) = \mathbf{E}_{x \sim p_{\text{data}}(x)} [\log D(x)] + \mathbf{E}_{z \sim p_z(z)} [\log(1 - D(G(z)))]$$

де: G – генератор, D – дискримінатор, $x \sim p_{\text{data}}(x)$ – розподіл реальних даних, $z \sim p_{\text{data}}(z)$ – розподіл генератора, x – вибірка з $p_{\text{data}}(x)$, z – вибірка з $p(z)$, $D(x)$ – дискримінатор мережі, $G(z)$ – генеративна мережа.

Дискримінатор навчається правильно класифікувати зображення об'єктів. Одночасно генератор намагається обійти класифікатор, змусивши його повірити, що приклади справжні. В результаті приклади, створені генератором, не відрізняються від справжніх даних, і дискримінатор завжди виводить з ймовірністю $1/2$ для кожного зображення, яке він виводить. В результаті, процес навчання GAN не потребує визначення градієнта статистичної суми.

Розглянутий підхід дозволяє збільшити набір зображень, запобігаючи навчанню нейронної мережі на невідповідних шаблонах, що може підвищити ефективність її моделі нейромережі за рахунок збільшення точності класифікації зображень об'єктів.

РОЗРОБЛЕННЯ ПРОТОТИПУ СПЕЦІАЛЬНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗОВАНОЇ ОБРОБКИ АЕРОЗНІМКІВ ДЛЯ БЕЗПЛОТНИХ АВІАЦІЙНИХ КОМПЛЕКСІВ КЛАСУ 1

За досвідом переважної більшості збройних конфліктів сучасності, зокрема й відсічі Україною збройної агресії Російської Федерації, найважливіша роль у системі бойового забезпечення військ належить розвідці. Серед усіх видів розвідки, які можуть застосовуватися у сучасних умовах підрозділами Збройних Сил (ЗС) України для з'ясування стану та положення військ (сил) противника, ключова роль належить повітряній розвідці засобами безпілотних авіаційних комплексів (БпАК). Ефективність ведення розвідки зазначеними засобами суттєво обмежується зростаючим обсягом розвідувальних матеріалів з БпАК в умовах часових і ресурсних обмежень та недосконалістю математичного забезпечення автоматизованої обробки добутих матеріалів. Існуюче наявне програмне забезпечення обробки аерознімків не є автоматичним, а тому має суттєві обмеження щодо його застосування на засобах БпАК. Це потребує впровадження нових підходів.

Найважливішим етапом, від якого залежить оперативність і достовірність інформації, що надається автоматизованою системою обробки, для прийняття рішення командирами відповідного рівня, є процес детального дешифрування об'єктів на аерознімках. При виконанні автоматизації даного етапу потрібно вирішити завдання виявлення, призначення точних обмежувальних рамок або масок для дрібнозернистих об'єктів та розпізнавання, відділення об'єктів переднього плану від фону і призначення їм відповідних міток класу об'єктів.

Існуючі автоматизовані засоби обробки і аналізу аерознімків, що побудовані на основі класичних методів розпізнавання образів, не дозволяють забезпечити необхідний рівень якості і оперативності розпізнавання зображень. Пріоритетним напрямом розв'язання проблеми забезпечення оперативності і якості розпізнавання вхідних образів є розробка моделей на основі штучних нелінійних нейронних мереж.

Для вирішення такого роду завдань на сучасному етапі розвитку інформаційних технологій широкого застосування набувають методи семантичної і елементної сегментації, розвиток яких на сьогодні відбувається паралельно один від одного, які мають свої особливості, переваги та недоліки. Тому актуальним завданням на сьогодні є пошук та удосконалення методів автоматичного дешифрування об'єктів на аерознімках, отриманих з безпілотних авіаційних комплексів, які б забезпечували достатню точність виявлення та розпізнавання об'єктів в складних топографічних умовах місцевості, над якими отримуються аерознімки.

Для вирішення цього завдання було удосконалено модель каскаду гібридної сегментації, що використовує комплексування різних підходів автоматичної обробки аерознімків. Ключовою ідеєю є поліпшення інформаційного потоку шляхом включення каскаду та багатозадачності на кожному його етапі та використання просторового контексту для подальшого підвищення точності виявлення та розпізнавання об'єктів. Нова структура дозволяє підвищити продуктивність проведенням багатоетапної обробки аерознімка, розрізняти різноплановий передній план від переповненого фону завдяки просторовому контексту, що надає використання семантичної сегментації.

Удосконалена модель каскаду сегментації враховує лінійні розміри шуканих об'єктів та їх співвідношення, можливу зміну масштабу, вплив топографічних елементів місцевості. Дана модель має стати основою для розробки спеціального програмного забезпечення автоматичного детального дешифрування об'єктів на аерознімках, отриманих з БпАК, та підвищити точність виявлення та розпізнавання об'єктів розвідки.

ТЕХНОЛОГІЯ SDN ТА МОЖЛИВОСТІ ЇЇ ВПРОВАДЖЕННЯ В МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Актуальність дослідження. У традиційній моделі мережеві провайдери змушені планувати кількість портів, комутаторів і маршрутизаторів з великим запасом, щоб покривати можливе різке зростання трафіку. У збройних силах кількість мережевого обладнання обмежена, а його стан та можливості не завжди можуть відповідати поставленим завданням. До того ж, оновлення програмного забезпечення і апаратних засобів іноді може викликати необхідність у придбанні додаткового обладнання та залучення додаткових спеціалістів, які займаються його підтримкою та налаштуванням програмного забезпечення, що функціонує в ІТ-середовищі. Це, в свою чергу, вимагає додаткових витрат та зумовлює затримки в оновленні мережевої інфраструктури. Таким чином, вивчення шляхів організації архітектури SDN-мереж є актуальним завданням.

Метою дослідження є проведення аналізу можливості підвищення ефективності мереж спеціального призначення за допомогою впровадження технології SDN.

Виклад основного матеріалу.

Одним з можливих варіантів вирішення більшості перерахованих проблем є застосування технології SDN, що дозволить змінити уявлення і суттєво вплинути на підхід до побудови мереж зв'язку. Теоретично SDN дає можливість абсолютної гнучкості в управлінні трафіком, легке балансування навантаженням без залучення окремого обладнання. Дані передаються відповідно до таблиць маршрутизації, що зберігаються на маршрутизаторах, але ці таблиці централізовано управляються віддаленою системою, у зв'язку з чим адміністратору не потрібно змінювати таблиці на кожному мережевому пристрої. В ідеальному випадку всі мережеві компоненти повинні управлятися і налаштовуватися в ході однієї операції. Спільна робота компонентів програмно-конфігурованої мережі може бути заснована на стандарті OpenFlow.

Гнучкість мережі SDN дозволить програмувати мережу як єдине ціле, а адміністраторам не доведеться займатися окремими пристроями. Реалізація концепції SDN на практиці дозволить адміністратору керувати всіма наявними мережевими пристроями, незалежно від виробника, а також налаштовувати роботу всієї мережі з одного робочого місця, що значно спростить її експлуатацію. Швидкість конфігурування мережі значно зросте, а параметри мережі можна буде оперативно змінювати в режимі реального часу, відповідно, терміни впровадження нових додатків і сервісів значно скоротяться.

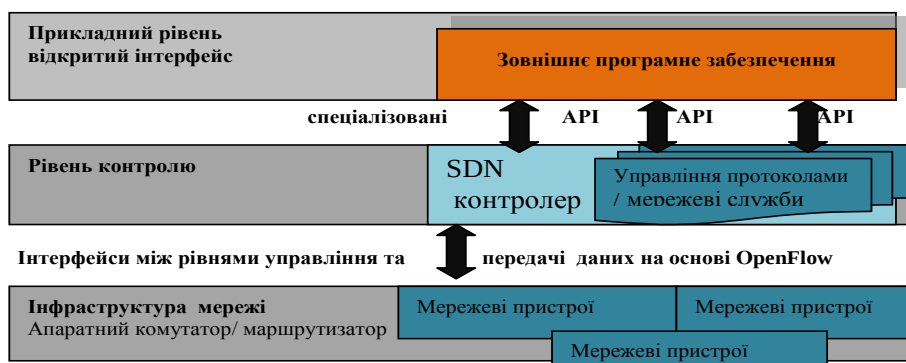


Рис. 1. Архітектура програмно-конфігурованої мережі

Висновки. Якщо порівнювати дану технологію з традиційною структурою мережі, що сьогодні ще залишається актуальною, то модель SDN має ряд переваг, серед яких розробники вирізняють такі: підвищення ефективності мережевого обладнання на 25-30 %; зниження на 30 % витрат на експлуатацію мереж; управління цілими мережами, а не мережевими пристроями; скоротити витрати на управління мережею.

МЕТОДИ ВІЗУАЛІЗАЦІЇ СТАТИСТИЧНИХ ДАНИХ ЗАСОБАМИ СУЧАСНИХ ВЕБ-ЗАСТОСУНКІВ

На сьогодні роль аналітичної складової сучасних систем обліку даних та вимоги до неї продовжують зростати. Прості та інформативні візуалізації допомагають ефективно обробляти великі масиви однотипних даних та швидко приймати рішення. Для користувачів систем візуалізації масивів даних важливим є наочність даної візуалізації та можливість індивідуального налаштування системи візуалізації згідно власних потреб для ефективної оцінки представленої інформації. Для постачальників інформації важливим є можливість ефективного внесення інформації в систему з мінімальним маніпулюванням над нею.

У ЗСУ продовжується процес впровадження інформаційних систем для підвищення ефективності управління та взаємодії. Саме тому зростає потреба в залученні систем візуалізації та статистичного аналізу наявної інформації для ефективного прийняття рішень на основі зібраних даних.

Для візуалізації інформації у веб-застосунках можуть використовуватися наступні методи:

1. Використання *DOM*-моделі.
2. Побудова *SVG*-графіки
3. Застосування технології *Canvas*

Використання *DOM* дозволяє будувати візуалізації зі строгою ієрархією представлення даних (звіти, таблиці), але водночас має обмежену кількість засобів для маніпуляції з графічним представленням даних (графіки, діаграми). *DOM*-модель є основою роботи сучасних браузерів, тому її досить легко впровадити і вона потребує мінімум зусиль для підтримання в актуальному стані. Важливою перевагою *DOM*-моделі є її сумісність з *CSS*-стилями, що в свою чергу дозволяє ефективно маніпулювати її зовнішнім виглядом.

Використання векторної графіки (*SVG*) дозволяє легко створювати графічні представлення певних наборів даних та взаємодіяти з ними. Так як для представлення *SVG*-графіки використовується формат *XML* – вона легко піддається машинній обробці, що дозволяє мінімізувати зусилля для створення простих візуалізацій на основі геометричних фігур та кривих описаних математичними функціями, або заданих набором точок на площині. Значною перевагою *SVG*-візуалізацій є сумісність цього формату з багатьма засобами перегляду зображень, що дозволяє легко експортувати текст в форматі *XML* в текстовий файл з розширенням *svg*. При цьому повністю зберігається вихідна якість візуалізації.

Застосування технології *Canvas* дозволяє створювати графічні візуалізації, що складаються з великої кількості деталей (як статичних, так і інтерактивних). Особливістю цієї технології є дуже розвинений *API*, що дозволяє ефективно використовувати її під час написання програмних додатків та візуалізаційних скриптів. Дуже ефективним є застосування цієї технології для побудови візуалізацій на основі карт та картограм. Водночас використання технології *Canvas* обмежене підтримкою стандарту *HTML5*, що унеможливорює її використання із застарілим обладнанням та програмним забезпеченням.

Таким чином дані технології можуть використовуватися для ефективного представлення різних типів даних з мінімальними зусиллями для впровадження й підтримки з боку розробників та використання з боку кінцевих користувачів. Комбіноване використання різних методів даних дозволяє створити максимально повну та інформативну систему візуалізації даних без втручання кінцевого користувача, додати можливість взаємодії з візуальними елементами для повного розуміння візуалізації і при цьому мінімізувати ресурси на її побудову та перегляд.

ПІДСИСТЕМА НАДАННЯ ДОСТУПУ ДО ІНФОРМАЦІЙНОГО СЕРВІСУ "АРМІЯ FM" В УМОВАХ НЕСТАБІЛЬНОГО З'ЄДНАННЯ З МЕРЕЖЕЮ НА ОСНОВІ КРОСС-ПЛАТФОРМЕННОГО МОБІЛЬНОГО ДОДАТКУ РОЗРОБЛЕНОГО НА ПЛАТФОРМІ FLUTTER

Актуальність роботи обумовлена необхідністю вдосконалення підсистеми надання доступу до інформаційного сервісу „Армія FM” в умовах нестабільного з’єднання з мережею і, як слідство, у підвищенні ефективності роботи розробленого мобільного додатку.

При розробці додатків необхідні враховувати деякі особливості: робота мобільних пристроїв здійснюється на автономних енергоносіях, що відображається на продуктивності роботи додатків. Крім цього, сучасні смартфони і планшети універсально мають додаткові пристрої, як гіроскопи, акселерометри і камери, які надають унікальні можливості для розширення функціональності програми. Як правило, продають мобільні пристрої з деякими, заздалегідь встановленими додатками. Сьогодні у кожної організації є вибір у вигляді розміщення інформації. Очевидно, що РС-версія сайту - це перше, що намагається створити організація, але зупинятися на цьому не варто. Крім того, розробивши мобільний додаток, яке містить весь вміст версії для ПК, можна отримати безліч переваг. Одним з них є то, що додаток можна завантажити тільки один раз на мобільний пристрій, і ви можете використовувати його в будь-який час в офлайн режимі. Використання додатків істотно позбавляє від довгих очікувань завантаження графіки, зображення, звуку та інших компонентів, а також економить час, оскільки програма вже встановлена на телефон і більшість елементів зберігаються в кеші. В цьому випадку кеш виступає в ролі центрального рівня зі своїм життєвим циклом і архітектурної топологією, і до нього можуть звертатися різнопланові системи додатку. Це особливо актуально для систем, в які динамічно масштабуються в обох напрямках. Розробники додатків можуть створювати мобільні додатки, які доступні для кожної операційної системи телефону або планшета як окремо, так і адаптувати розробку для всіх видів відомих на сьогодні операційних систем для мобільних пристроїв, за допомогою автоматизованого інструментарію. Сьогодні мобільний додаток має особливе значення для компаній, які в своїй діяльності приділяє велику увагу використанню Інтернету та роботі з широким колом користувачів. Поліпшення програми та зміцнення авторитету і репутації компанії взаємопов’язані.

Сучасний етап розвитку систем доступу до мережі Інтернет та обробки інформації характеризується розширенням галузей застосування, в значній частині з яких вимагається опрацювання за складними алгоритмами у реальному часі різних за інтенсивністю надходження потоків даних як на комп’ютерних засобах так і мобільних пристроях, що повинні задовольняти обмеженням щодо габаритів, енергоспоживання, вартості та часу розробки систем. Режим реального часу накладає обмеження на час обробки інформації, який не повинен перевищувати часу обміну даними.

На практиці для реалізації алгоритмів надання доступу до мережі та обробки інформації у реальному часі використовуються комбіновані підходи. Вибір тої чи іншої бібліотеки як основної для реалізації алгоритмів здійснюється із вимог забезпечення максимально високої стабільності роботи системи відносно зворотнопропорційної якості з’єднання з мережею та високої ефективності використання програмного та технічного забезпечення. У системах надання доступу до мережі та обробки інформації у режимі реального часу забезпечується розпаралелюванням і конвеєризацією процесів обробки. В зв’язку з цим актуальною задачею є

розробка вискоєфективної підсистеми надання доступу до інформаційного сервісу через мережу Інтернет.

Метою дослідження є вибір принципів і засобів реалізації, визначення основних шляхів підвищення ефективності підсистеми, використання вбудованих бібліотек та методів роботи з мережею, розроблення методів вискоєфективної взаємодії користувача з мережею управління та обробки сигналів у реальному часі за рахунок виконання **наступних часткових завдань дослідження**:

- аналіз сучасних підходів у створенні мобільних додатків для загального використання, спираючись на вимоги керівних документів;
- вдосконалення самого алгоритму надання доступу до мережі та процесів, що пов'язані з цією задачею, з урахуванням недоліків та обмежень сучасної моделі;
- розширення функціоналу додатку враховуючи потреби Збройних Сил та цивільного населення. Адаптація його роботи в усіх напрямках з метою взаємодії військових та цивільного населення

Виклад основного матеріалу. В історії є безліч прикладів, коли інформаційна боротьба вирішувала фінал на полі бою. Ще з часів козацтва діяла так звана практика поширення інформації серед населення та ворожого війська з метою агітації або залякування. В часи другої Світової війни психологічна боротьба перейшла на новий рівень, саме в той час для так званої інформаційної війни, окрім усної передачі та друкованих видань почало використовуватись радіо та телебачення.

В час, коли в нашій державі ведеться інформаційна війна та існує відкритий конфлікт, доступ до достовірної інформації є надзвичайно важливим. Саме це є одним з головних завдань інформаційного сервісу „Армія FM”, що веде свою діяльність саме для військових. Даний сервіс окрім надання доступу до політично нейтральних новин ставить завдання створення полігону для взаємозв'язку між військовослужбовцями та цивільним населенням, підвищення морально-психологічного та патріотичного стану, інформаційної освіченості та громадянської свідомості.

На даний момент алгоритми надання доступу при умовах нестабільного з'єднання з мережею, мають ряд недоліків. Саме тому постає мета удосконалення підсистеми надання доступу до інформаційного сервісу „Армія FM” в умовах нестабільного з'єднання з мережею.

Для розробки на платформі Flutter мовою Dart існує безліч бібліотек та програмних рішень для роботи з мережею та даними. Що дає змогу створювати гнучкі та ефективні алгоритми для функціонування системи надання доступу в умовах нестабільного з'єднання з мережею. Після проведеного аналізу та співставлення попередніх версій системи та іноваційних рішень платформи Flutter, що активно розвивається, було виявлено помилки, неактуальні та застарілі програмні рішення.

Базуючись на проведеній роботі, використовуючи новітній підхід проектування та останні тенденції розробки на платформі Flutter було розроблено узагальнену архітектуру і алгоритми роботи підсистеми надання доступу до інформаційного сервісу „Армія FM” в умовах нестабільного з'єднання з мережею.

Під час оцінки ефективності отримано приблизний результат затрат часу на встановлення з'єднання. Після проведення тестувань розробленого алгоритму, розробленому алгоритму було надано високу оцінку стійкості до відмов, тобто дана підсистема доступу допускає 2% відмов на 1000 сесій.

Висновки. Отже, в роботі розроблене архітектурне та програмне рішення підсистеми доступу до інформаційного сервісу „Армія FM” та на її основі реалізовано кросс-платформенний мобільний додаток надання доступу до інформаційного сервісу «Армія FM».

ВАРІАНТ ОЦІНКИ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ ВІЙСЬКОВОГО РАДІОЗВ'ЯЗКУ В УМОВАХ РАДІОЕЛЕКТРОННОГО ПОДАВЛЕННЯ

Сучасні системи передачі інформації здійснюють інформаційне забезпечення значної кількості стаціонарних та рухомих користувачів, доволіно розташованих в межах певної території. Внаслідок чого альтернативи системам радіозв'язку не має. Одна з технологій радіозв'язку передбачає багатоадресний доступ в загальному частотному каналі, при якому користувачі незалежно один від одного передають та приймають інформацію за необхідністю. Характерними перевагами радіозв'язку є: швидке встановлення зв'язку на значні відстані; висока мобільність та можливість забезпечення зв'язку на складному рельєфі місцевості. Визначення ефективності функціонування системи військового радіозв'язку пов'язана із зазначеними вище особливостями та наявністю декількох технологій формування та обробки радіосигналів. При цьому виникає необхідність обчислення кількісної оцінки впливу завад (засобів радіоелектронного подавлення) на систему військового радіозв'язку.

Шляхи підвищення ефективності систем радіозв'язку на основі того або іншого критерію шляхом оптимізації за рядом параметрів розглянуто в роботах [1 – 3]. У роботі [4] в якості міри ефективності системи, використовується аналіз потоків інформації, що передаються через вузли системи. Відомо, що системи військового призначення функціонують в умовах активного радіоелектронного придушення з боку противника. Дана обставина обов'язково повинна враховуватися при оцінці ефективності функціонування реальної системи радіозв'язку. Тому, запропоновано варіант оцінки ефективності системи військового радіозв'язку, що функціонує в умовах радіоелектронного подавлення. Реалізація даного варіанту включає наступну послідовність дій:

1. Формування даних про елементи системи (технічні характеристики засобів передачі інформації, використовуваних у системі; топологія системи; координати вузлів, складання інформаційної матриці системи).
2. Формування даних про засоби радіоелектронного подавлення (технічні характеристики та координати позицій).
3. Розрахунки співвідношень “сигнал – завада + шум” на вході кожного приймального пристрою засобу передачі інформації.
4. Оцінка ступеню погіршення пропускної здатності системи в обраній ланці управління або в системі в цілому.
5. Оцінка частини інформації, яка циркулює в обраній ланці управління (при необхідності). Якщо оцінка здійснюється за систему в цілому.
6. Розрахунки ефективності системи.

Таким чином, запропоновано варіант оцінки ефективності системи військового радіозв'язку в умовах радіоелектронного подавлення, який може слугувати основою для розробки удосконаленої методики забезпечення завадозахищеного військового радіозв'язку.

ЛІТЕРАТУРА

1. Цибизов А. А. Оценка эффективности сетей связи. Вестн. Рязанского РГРТУ. 2009. № 3(29). С. 18 – 22.
2. Медведев Н. В., Свистун А. И. Формализация показателей качества функционирования телекоммуникационных сетей нового поколения. Наука и образование. 2016. № 7. С. 267 – 273.
3. Ипатов В. П. Широкополосные системы и кодовое разделение сигналов. / Ипатов В. П. – М.: Техносфера, 2007. – 488 с.
4. Srikant, R. & Lei, Ying. (2014). Communication Networks: An optimization, control, and stochastic networks perspective. Cambridge Univ. Press.

АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ – ОСНОВА ЕФЕКТИВНОГО ЗАХИСТУ ПІДПРИЄМСТВА

Актуальність Сьогодні інформаційні системи (ІС) відіграють ключову роль в забезпеченні ефективності роботи комерційних і державних підприємств. Повсюдне використання ІС для зберігання, обробки і передачі інформації робить актуальними проблеми їх захисту, особливо з огляду на глобальну тенденцію до зростання числа інформаційних атак, що приводять до значних фінансових і матеріальних втрат. Для ефективного захисту від атак компаніям необхідна об'єктивна оцінка рівня безпеки ІС - саме для цих цілей і застосовується аудит безпеки.

Визначення аудиту безпеки ще не усталене, але в загальному випадку його можна описати як процес збору та аналізу інформації про ІС для якісної або кількісної оцінки рівня її захищеності від атак зловмисників. Існує безліч випадків, коли доцільно проводити аудит безпеки. Це робиться, зокрема, при підготовці технічного завдання на проектування і розробку системи захисту інформації та після впровадження системи безпеки для оцінки рівня її ефективності. Можливий аудит, спрямований на приведення діючої системи безпеки у відповідність вимогам законодавства. Аудит може також призначатися для систематизації та впорядкування існуючих заходів захисту інформації або для розслідування інциденту, що стався, пов'язаного з порушенням інформаційної безпеки.

Як правило, для проведення аудиту залучаються зовнішні компанії, які надають консалтингові послуги в області інформаційної безпеки. Ініціатором процедури аудиту може стати керівництво підприємства, служба автоматизації або служба інформаційної безпеки. У ряді випадків аудит також проводиться на вимогу страхових компаній або регулюючих органів. Аудит безпеки виконується групою експертів, чисельність і склад якої залежить від цілей і завдань обстеження, а також від складності об'єкта оцінки.

Можна виділити наступні основні види аудиту інформаційної безпеки:

експертний аудит безпеки, в ході якого виявляються недоліки в системі заходів захисту інформації на основі досвіду експертів, що беруть участь в процедурі обстеження;

оцінка відповідності рекомендаціям міжнародного стандарту ISO/IES 27001 та інших стандартів,

інструментальний аналіз захищеності ІС, спрямований на виявлення та усунення вразливостей програмно-апаратного забезпечення системи;

комплексний аудит, який включає в себе всі перераховані вище форми проведення обстеження [1].

Будь-який з перерахованих видів аудиту може проводитися окремо або в комплексі, в залежності від тих завдань, які вирішує підприємство. Як об'єкт аудиту може виступати як ІС компанії в цілому, так і її окремі сегменти, в яких обробляється інформація, що підлягає захисту.

Який би вид аудиту інформаційної безпеки не був проведений, кінцевим результатом мають бути розроблені рекомендації щодо вдосконалення організаційно-технічного забезпечення захисту на підприємстві. Такі рекомендації можуть включати в себе різні типи дій, спрямованих на мінімізацію виявлених ризиків [2]:

1. Зменшення ризику за рахунок додаткових організаційних і технічних засобів захисту, що дозволяють знизити ймовірність проведення атаки або зменшити можливі збитки від неї. Так, установка міжмережевих екранів в точці підключення ІС до Інтернету істотно знижує ймовірність проведення успішної атаки на загальнодоступні інформаційні ресурси ІС - такі, як Web-сервери, поштові сервери і т. Д.

2. Ухилення від ризику шляхом зміни архітектури або схеми інформаційних потоків ІС, що дозволяє виключити проведення тієї чи іншої атаки. Наприклад, фізичне відключення від

Інтернету сегмента ІС, в якому обробляється конфіденційна інформація, дозволяє уникнути зовнішніх атак на конфіденційну інформацію.

3. Зміна характеру ризику в результаті вживання заходів по страхуванню. Як приклади зміни характеру ризику можна привести страхування обладнання ІС від пожежі або страхування інформаційних ресурсів від можливого порушення їх конфіденційності, цілісності або доступності. В даний час ряд російських компаній вже пропонують послуги страхування інформаційних ризиків.

4. Прийняття ризику, якщо він зменшений до того рівня, на якому вже не представляє небезпеки для ІС.

Зазвичай рекомендації спрямовані не на повне усунення всіх виявлених ризиків, а лише на їх зменшення до прийняттого рівня. При виборі заходів для підвищення рівня захисту ІС враховується одне принципове обмеження - вартість реалізації цих заходів не повинна перевищувати вартості захищаються інформаційних ресурсів, а також збитків компанії від можливого порушення конфіденційності, цілісності або доступності інформації.

На завершення процедури аудиту його результати оформляються у вигляді звітнього документа, який надається замовнику. У загальному випадку цей документ складається з наступних основних розділів [3]:

- опис меж, в рамках яких проводився аудит безпеки;

- опис структури ІС замовника;

- методи і засоби, які використовувалися в процесі проведення аудиту;

- опис виявлених вразливостей і недоліків, включаючи рівень їх ризику;

- рекомендації щодо вдосконалення комплексної системи забезпечення інформаційної безпеки;

- пропозиції до плану реалізації першочергових заходів, спрямованих на мінімізацію виявлених ризиків.

Висновок

Аудит інформаційної безпеки – один з найбільш ефективних сьогодні інструментів для отримання незалежної і об'єктивної оцінки поточного рівня захищеності підприємства від загроз інформаційної безпеки. Крім того, результати аудиту дають основу для формування стратегії розвитку системи забезпечення інформаційної безпеки організації. Однак необхідно розуміти, що аудит безпеки – не разовий процедура, він повинен проводитися на регулярній основі. Тільки в цьому випадку аудит буде приносити реальну віддачу і сприяти підвищенню рівня інформаційної безпеки компанії.

ЛІТЕРАТУРА

1. Аверченко, В.І. Аудит інформаційної безпеки: навч. посібник для вузів / – Брянськ: БГТУ, 2005.
2. Милославська Н.Г. Перевірка і оцінка діяльності з управління інформаційною безпекою. – М., 2012.
3. Філіпів Д.Ю. Внутрішній аудит: міфи і реальність // Облік і контроль. 2007. № 1.

ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ CAPACITY PLUS MULTI-SITE MOTOTRBO™ ДЛЯ ПОБУДОВИ СИСТЕМИ ТРАНКІНГОВОГО ЗВ'ЯЗКУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Платформа MOTOTRBO™ розроблена у відповідності до Європейського стандарту цифрового рухомого радіозв'язку Digital Mobile Radio (DMR), основні засади якого зазначені у документах ETSI 102361-1/2/3.

Радіозасоби MOTOTRBO™ можуть забезпечувати такі основні функції: індивідуальні виклики; групові виклики; динамічне перегрупування користувачів та груп користувачів; переадресація виклику від радіотерміналу; управління сеансами зв'язку; забезпечення екстрених викликів; виклики до відомчих мереж; обмін у групі; втручання, при наявності права, у діючу розмову; пріоритетне сканування; віддалене управління терміналами; забезпечення виклику через диспетчера; забезпечення ідентифікації, реєстрації та утримання виклику тощо. Перелік можливостей, що підтримуються в окремій радіомережі, залежить від технології її організації.

На даний час у Збройних Силах України для побудови територіально рознесених транкінгових радіомереж застосовується технологія IP Site Connect на основі радіозасобів MOTOTRBO™, яка дозволяє поєднувати між собою ретранслятори на основі IP-мережі. При цьому, для побудови декількох радіомереж необхідно розгортати окремі мережі ретрансляторів. На окремих ретрансляторах окремої мережі використовується лише один канал на прийом і один на передачу, що обмежує одночасну передачу повідомлень на окремих напрямках до одного та не забезпечують більшість потенційних можливостей радіозасобів MOTOTRBO™.

Використання технології IP Site Connect з обмеженням можливостей одночасних передач повідомлень при збільшенні кількості радіостанцій в окремих мережах призводить таких негативних наслідків: колізій і затримок в передачі повідомлень (розмовних та даних), підвищених витрат заряду батарей радіостанцій, підвищеного використання радіочастотного ресурсу, обмежень в використанні потенційних можливостей радіостанцій MOTOTRBO (до 15%) тощо.

Для організації систем транкінгового зв'язку спеціального призначення пропонується використовувати технологію Capacity Plus Multi-Site, яка дозволяє створити єдину мережу сайтів (базових станцій) в інтересах декількох окремих структур/підрозділів/груп абонентів з розгортанням декількох ретрансляторів на окремих сайтах (до 15) з можливістю надання, відповідно, декількох каналів для організації зв'язку з автоматичним виділенням вільного каналу.

Використання технології Capacity Plus Multi-Site надає такі переваги:

- можливість розгортання єдиної радіомережі для декількох окремих груп абонентів;
- підвищення можливої кількості радіо абонентів в мережі;
- підвищення кількості одночасних розмов в окремих структурах/підрозділах/групах абонентів в межах одного та декількох сайтів;
- зменшення використання радіочастотного ресурсу;
- зменшення використання антено-щоголового, фідерного обладнання, обладнання безперебійного електроживлення та іншого обладнання сайтів (базових станцій);
- підвищення використання можливостей радіозасобів MOTOTRBO™ до 75 %;
- централізоване керування єдиною радіомережею як загальне, так і в інтересах окремих груп абонентів.

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ПОЄДНАННЯ СИСТЕМ ПОПЕРЕДЖЕННЯ ТА ВИЯВЛЕННЯ ВТОРГНЕНЬ

Актуальність. Разом із значним збільшенням кількості підключень до Інтернету та використанням широкосмугових та мобільних технологій, спостерігається величезне збільшення кількості комп'ютерних систем та пристроїв зберігання даних, підключених до мережі загального користування. З постійно зростаючою залежністю від обчислювальної інфраструктури, критичні ІТ-активи, конфіденційні дані та інтелектуальна власність піддаються кібератакам. У відповідь на постійні зміни векторів кіберзагроз, було розроблено та впроваджуються системи запобігання вторгнень, які забезпечують додатковий захист, на додавання до існуючого, з використанням брандмауерів, систем виявлення вторгнень та інших засобів захисту інформації в ІТС.

Мета. Метою роботи є дослідження ефективності поєднання методів аналізу систем попередження та виявлення вторгнень.

Основна частина. На сьогоднішній день, з'явилися інтерфейси для підвищення точності у використанні HIPS та NIPS. Коли NIPS бачить шкідливу подію, HIPS може підтвердити це, і навпаки. Наприклад, якщо пристрій NIPS виявляє атаку на служби HTTP, він може запитати HIPS, що працює на хості, чи працює саме ця веб-служба. У разі позитивної відповіді атака підтверджується. Якщо навпаки, атака позначається як помилковий сигнал тривоги.

Іншим прикладом може бути випадок, коли HIPS бачить аномальну мережеву активність на хості. HIPS консулюється з NIPS, щоб визначити, чи є діяльність небезпечною. NIPS може повідомити про те, що хост, з якого проходить активність, нещодавно був ідентифікований як зловмисник. Тоді HIPS знає, що аномальна активність є реальною атакою і відповідає належним чином.

В даний час розроблюються та впроваджуються продукти, які можуть читати системні журнали, журнали програм та події IPS та співвідносити їх між собою, щоб допомогти у дослідженні атак. Результатом таких заходів є менша кількість помилково позитивних подій із пристроїв безпеки та краще розуміння того, що означають різні випадки подій, якщо розглядати їх як сукупну картину стану мережі.

Ця ж концепція застосовується до комп'ютерної безпеки. Надалі, кожен елемент може ділитися інформацією з усіма іншими. Наприклад, брандмауер, NIPS та HIPS виявляють підозрілу, але потенційно небезпечну розвідувальну діяльність, що походить від одного хоста. Усі вони повідомляють про свої висновки на одному пристрої для збору та кореляції. Пристрій бачить три подібні звіти та надсилає повідомлення назад, вказуючи на те, що розвідувальні заходи дійсно ведуться і що нападаючого хоста слід уникати.

У майбутньому контрзаходи безпеки зможуть вживати спільних, а не індивідуальних дій під час інциденту. У випадку, коли IPS виявляє атаку, він вживає заходів відповідно до своїх налаштувань конфігурації. Коли IPS виявляє атаку, що походить від внутрішнього хоста, він може вжити звичайних дій, а також налаштувати мережу для попередження атаки. Маршрутизатори, комутатори та брандмауери будуть переналаштовані IPS, щоб переконатися, що атака не буде поширюватися по всій мережі.

Висновок. HIPS та NIPS можуть працювати разом, щоб налаштувати один одного. Наприклад, якщо HIPS бачить атаку на захищений хост, він може повідомити NIPS. NIPS може прийняти це повідомлення та переконафігурувати себе, щоб вжити більш жорстких заходів проти трафіку зловмисника. Крім того, якщо функціональність IPS інтегрована у безліч різних пристроїв в мережі (таких як брандмауери та маршрутизатори), усі ці пристрої можуть спільно брати участь для забезпечення безпеки у мережі.

ПРОЕКТ СТАНДАРТУ АВТЕНТИФІКАЦІЇ, ЯКИЙ МОЖНА АДАПТУВАТИ ДЛЯ ВИКОРИСТАННЯ В ПОСТКВАНТОВИЙ ПЕРІОД

Проект нового національного стандарту автентифікації було розроблено на замовлення ДССЗЗІ у ході виконання НДР.

Проект стандарту містить дві версії протоколу автентифікації – повну та скорочену. Скорочена версія використовується у тому випадку, коли двом сторонам – учасникам протоколу – потрібно лише підтвердити особистість один одного. Повна версія використовується у тому випадку, коли сторонам, крім підтвердження особистості, потрібно також виробити:

- спільні ключі для MAC-кодів,
- спільні ключі для вибраного алгоритму шифрування;
- спільні вектори ініціалізації для цього ж алгоритму.

Повна версія протоколу складається з 15 кроків, які наведено нижче.

Крок 1. Передавання підписаного відкритого ключа Клієнта та випадкового рядка.

Крок 2. Передавання підписаного відкритого ключа Сервера та випадкового рядка.

Крок 3. Перевірка правильності повідомлення, відправленого Сервером на Кроці 2, та підпису на ньому.

Крок 4. Перевірка правильності повідомлення, надісланого Клієнтом на Кроці 1, та підпису на ньому.

Крок 5. Надсилення Клієнтом Серверу своєї частини секрету.

Крок 6. Надсилення Сервером Клієнту своєї частини секрету.

Крок 7. Перевірка Клієнтом формату повідомлення, надісланого Сервером на Кроці 6, коректності підпису на ньому та обчислення Клієнтом значення *PreMasterSecret*.

Крок 8. Перевірка Сервером формату повідомлення, надісланого Клієнтом на Кроці 5, коректності підпису на ньому та обчислення Сервером значення *PreMasterSecret*.

Крок 9. Обчислення Клієнтом значення *MasterSecret*.

Крок 10. Обчислення Сервером значення *MasterSecret*.

Крок 11. Обчислення Клієнтом ключів для MAC-кодів, ключів для вибраного алгоритму шифрування та векторів ініціалізації для цього ж алгоритму.

Крок 12. Обчислення Сервером ключів для MAC-кодів, ключів для вибраного алгоритму шифрування та векторів ініціалізації для цього ж алгоритму.

Крок 13. Обчислення Клієнтом шифртексту від конкатенації всіх повідомлень протоколу.

Крок 14. Перевірка Сервером правильності зашифрованого повідомлення, надісланого Клієнтом на Кроці 13, та обчислення Сервером шифртексту від конкатенації всіх повідомлень протоколу.

Крок 15. Перевірка Клієнтом правильності зашифрованого повідомлення, надісланого Сервером на Кроці 14, та підтвердження взаємної автентифікації.

Вкорочений протокол складається з 11 кроків (перші 8 з них однакові в обох версіях протоколу) та закінчується лише взаємною автентифікацією, без вироблення ключів та векторів ініціалізації.

Криптографічні механізми, що використовуються у протоколі, базуються на останніх досягненнях у галузі криптології, зокрема посилаються на нові національні стандарти. Запропонований у проекті протокол автентифікації може бути адаптований для використання в постквантовий період, якщо для цифрового підписування та обміну ключами використовуються перетворення, що є стійкими в постквантовий період.

АЛГОРИТМ ПОБУДОВИ МАРШРУТУ ПОЛЬОТУ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ І КЛАСУ У СКЛАДНИХ УМОВАХ

Досвід бойових дій на сході України проти російського агресора показав, що противник активно застосовує засоби радіоелектронної боротьби (РЕБ) Вони спроможні відстежувати та подавляти канали управління безпілотних літальних апаратів (БпЛА) на маршруті польоту. Подавлення каналу управління засобами РЕБ здатне, як мінімум, перешкодити виконанню завдання повітряної розвідки.

На даний час зафіксовано багато випадків впливу засобів РЕБ противника на БпЛА І класу шляхом створення шумових перешкод каналів управління та приймачів GPS. У зоні проведення ООС розвідувальними підрозділами Збройних Сил України було виявлено станції виробництва Російської Федерації (РФ) типу Р-330Ж „Житель”, 1Л-262 „Ртуть-БМ”, РБ-341В „Леер-3”. З метою недопущення втрат БпЛА через вплив ворожих засобів РЕБ актуальним та нагально необхідним є питання розробки нових та вдосконалення існуючих алгоритмів побудови маршруту БпЛА І класу в умовах складної радіоелектронної обстановки, що дозволить підвищити ефективність їх застосування під час виконання бойових завдань.

На сьогоднішній день питання захисту БпЛА від засобів РЕБ частково вирішене шляхом, виконання корпусу літального апарата із спеціального покриття, яке ускладнює виявленням БпЛА технічними та радіотехнічними засобами розвідки, використовуються закриті канали зв'язку, проводиться їх кодування, шифрування з обов'язковим дублюванням і резервуванням бортових систем та підсистем управління, використанням різних систем навігації, підвищенням «інтелекту» БпЛА щодо автономних дій.

З метою подальшого розвитку систем захисту БпЛА від РЕБ існує необхідність побудови оптимального маршруту польоту БпЛА, який залежатиме від рельєфу місцевості де буде здійснюватися повітряна розвідка БпЛА, визначення всіх метрологічних умов, та визначення місця знаходження, радіус дії засобів РЕБ із використанням даних космічної розвідки.

Дана послідовність операцій щодо планування маршруту польоту дасть змогу отримувати точні координати станцій РЕБ противника, а також прогнозувати їх можливості щодо подавлення.

Також необхідно відмітити доцільність проведення аналізу тактико-технічних характеристик БпЛА на ступінь їх вразливості подавленню різних типів вітчизняних станцій РЕБ для формування розуміння ступеню їх захищеності та готовності до роботи у режимі подавлення.

Для реалізації цього варто передбачити функцію в якій оператор-пілот БпЛА зможе обрати тип техніки РЕБ, які є на озброєнні РФ, і в автоматичному режимі прорахувати радіус дій, всі діапазони частот на яких вони працюють з метою побудови максимально безпечного маршруту польоту БпЛА.

Запропоновані підходи можна реалізувати за рахунок комплексування даних від різних джерел розвідки, а особливо при взаємодії зі своїми підрозділами радіо-електронної розвідки. Такий алгоритм дасть можливість знизити ризик потрапляння БпЛА під дію ворожих засобів РЕБ противника в зоні бойових дій на сході України.

АНАЛІЗ МЕТОДІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМ АВТОМАТИЧНОГО КЕРУВАННЯ АКТИВНИХ ФАЗОВАНИХ АНТЕН

Розвиток теорії і практики проектування антенних систем пов'язаний із зростанням їх ролі в радіотехнічних системах різного призначення. Аналіз технічних характеристик сучасних антен і досвід їх використання в різних радіосистемах показав, що найповніше вимогам до антенних систем радіоапаратури багатофункціонального призначення відповідають активні фазовані антенні решітки (АФАР). Данні антенні системи широкого використовуються у складі бортових і наземних радіолокаційних станцій, радіонавігації, у якості антен радіосистем для зв'язку з безпілотними літальними апаратами.

Основними перевагами і можливостями АФАР є: підвищена швидкодія із-за можливості застосування малопотужних напівпровідникових фазообертачів і наявністю додаткового керування рівнем амплітуди на виході приймально-передавального модулю (ППМ) за рахунок регулювання коефіцієнта передачі підсилювальних каскадів, що в цілому дозволяє в режимі передачі швидко змінювати амплітудно-фазовий розподіл АФАР хвиль збудження по апертурі, таким чином і характеристики випромінювання; високий рівень випромінюваної потужності, який забезпечується просторовою сумою сигналів ППМ різних каналів, що дозволяє отримати рівень випромінюваної потужності, набагато більший за рівень потужності одиночного фідерного тракту; можливість компенсації втрат в розподільних системах і фазообертачах; підвищена експлуатаційна надійність із-за збільшеної кількості активних елементів антенних решіток.

Реалізація високих потенційних можливостей АФАР, як антенної системи радіоапаратури багатофункціонального призначення, неможлива без ретельного аналізу змін її характеристик при зміні режимів роботи з урахуванням всіх особливостей електродинамічних процесів, що відбуваються. Для забезпечення безперервного, швидкого та точного керування параметрами АФАР необхідно побудувати систему автоматичного керування (САК) у відповідності до вимог, що висуваються до цих систем. Для визначення показників якості САК АФАР використовуються прямі та безпосередні методи аналізу їх якості. Прямими називаються методи, які дозволяють дослідити якість систем автоматичного керування на основі аналізу реакції САК на зовнішні впливи шляхом вирішення диференційного рівняння математичної моделі САК, а також знаходження інтегралу згортки. Безпосередніми називаються методи, що дозволяють дослідити якість САК без визначення реакції САК на зовнішні впливи. Із безпосередніх методів найбільше застосовується метод коефіцієнтів помилок, частотний метод і метод інтегральних оцінок. Перевагою безпосередніх методів у порівнянні із прямими полягає у простоті їх застосування і можливість порівняно простої оцінки впливу параметрів системи на її якість.

Аналіз існуючих методів підвищення ефективності функціонування САК АФАР показав, що найбільш простими і прозорими є безпосередні методи, серед яких частотний метод, коефіцієнтів помилок, квадратичних інтегральних оцінок. Але використання безпосередніх методів не завжди доцільно для випадків, коли не можливо з максимальною точністю визначити в якому саме елементі структурної схеми змодельованої системи надходить збурююча дія, тобто має випадковий характер. Вирішення даного завдання має два шляхи: використання прямих методів; побудова еквівалентної САК з діаграмою направленості (ДН) АФАР за задаючою і збурюючою дією. Така САК дозволить не лише оцінити, а й керувати параметрами ДН АФАР в реальному часі. Тому предметом досліджень буде метод підвищення швидкодії та динамічної точності САК ДН АФАР в умовах випадкових задаючих і збурюючих впливів за допомогою нейронної мережі.

СТРУКТУРА УДОСКОНАЛЕННЯ МЕТОДУ АНАЛІЗУ І ОЦІНЮВАННЯ ШКОДИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ У РАЗІ ВИТОКУ ДЕРЖАВНОЇ ТАЄМНИЦІ

Актуальність. З огляду на наявність з 2014 року тимчасово окупованої території України та районів проведення антитерористичної операції (АТО), вже з 2018 року операції об'єднаних сил (ООС), гостро постає питання щодо необхідності забезпечення охорони державної таємниці (ОДТ) від терористичних загроз. У якості таких заходів щодо зміцнення національної безпеки України, враховуючи ситуацію, що склалася у східних регіонах України, з метою підвищення готовності до відвернення і нейтралізації загроз, забезпечення протидії терористичним проявам та вдосконалення механізму вироблення і реалізації єдиної державної політики у сфері цивільного захисту, стало прийняття рішень РНБО України „Про додаткові заходи щодо зміцнення національної безпеки України” та „Про стан подолання негативних наслідків, спричинених втратою матеріальних носіїв секретної інформації на тимчасово окупованій території України, в районі проведення антитерористичної операції в Донецькій та Луганській областях”, зокрема, щодо запровадження критеріїв класифікації, оцінки та ідентифікації рівнів терористичних загроз, визначення з урахуванням цих рівнів комплексу заходів із запобігання, реагування і припинення терористичних актів, установлення режимів контролю, охорони та захисту об'єктів можливих терористичних посягань залежно від категорії об'єкта. Також з 2020 року були внесені зміни до „Звіту про стан забезпечення ОДТ” (далі – Звіт) [1], який містить динамічно-змінювані набори ідентифікуючих та оціночних параметрів для оцінювання можливої шкоди національній безпеці України у разі витоку державної таємниці (ДТ), що тим чи іншим чином вносить корективи та доповнення до окремих кроків виконання розробленого методу аналізу і оцінювання шкоди національній безпеці України у разі витоку ДТ [2]. Окрім цього, з 2016 року введено порядок формування переліку інформаційно-телекомунікаційних систем (ІТС), що обробляють інформацію з обмеженим доступом, у тому числі і таємну, як критичної інформаційної інфраструктури держави, з урахуванням негативних наслідків, до яких може призвести кібератака на ці ІТС. Саме тому, удосконалення методу аналізу і оцінювання шкоди національній безпеці України у разі витоку ДТ є актуальним завданням.

Мета. Виходячи з викладеного, метою роботи є удосконалення методу аналізу і оцінювання шкоди національній безпеці України у разі витоку ДТ у частині оновлення набору ідентифікуючих та оціночних параметрів для оцінювання величини можливої шкоди у відповідності до Звіту та існуючих законодавчих вимог у сфері ОДТ, кібербезпеки та захисту інформації з урахуванням рівня терористичних загроз як для окремих тимчасово окупованих територій, так і для держави в цілому.

Основні положення. Розроблено нову структуру удосконалення методу аналізу і оцінювання шкоди національній безпеці у разі витоку ДТ, яка у порівнянні від існуючого [2], сформована з п'яти етапів, кожен з яких має різну кількість кроків. У таблиці 1 приведено порівняльну структуру методу, загальну характеристику, назву нового кроку та етапів його удосконалення.

Таблиця 1

**Порівняльна таблиця існуючого та удосконаленого
методу аналізу і оцінювання шкоди національній безпеці України у разі витоку ДТ**

Структура існуючого методу [2]	Структура удосконаленого методу
Крок 1. Ідентифікація події та атак: $A \in \{a_1, \dots, a_j\}$, $A = \{a_j\}$, $j = \overline{1, l}$. $E = \{E_1, E_2\}$, E_1 – „Розголошення (Р)”; E_2 – „Втрата (В)”.	<i>Етап 1. Аналіз стану забезпечення ОДТ.</i>
Крок 2. Ідентифікація відомостей, що становлять ДТ: $x_i \in PV_{N.i.j}$, де PV – короткий зміст відомостей x_i , N – сфера	Крок 1.1. Відомості про суб'єкта звітності (ОКІ), його підпорядкування та відомчу незалежність.
ДТ, як $N \in \{N_1, N_2, \dots, N_v\}$ (v – кількість сфер).	Крок 1.2. Відомості про РСО, фінансування заходів ОДТ.
	Крок 1.3. Відомості щодо наявності у працівників допуску та доступу до ДТ.
	Крок 1.4. Відомості про кількість матеріальних носіїв секретної інформації.

Крок 3. Розрахунок коефіцієнта важливості за СС відомостей: $\beta = w(x_i)/W(X) = w(PV_{N,i,j}) / \sum_{i=1}^y w(PV_{N,i,j}), i = \overline{1, y},$ Крок 4. Розрахунок коефіцієнта захищеності відомостей: $\Upsilon = \beta_x / A_j , j = \overline{1, I}, K_{ziN} = \Upsilon \cdot P^T.$ Крок 5. Розрахунок рівня зниження ефективності складової частини об'єкта (СЧО): $K^{\text{содт}} = 1 - \rho, \rho = 1 - (W(X) - w(x_i)) / W(X).$ Крок 6. Розрахунок відносної вартості СЧО: $\langle BVCCHO, k_{BVCCHO}, X_{BVCCHO}, \overline{k_{BVCCHO}} \rangle, \\ \overline{k_{OCP}}; \overline{k_{CCP}}; \overline{k_{OP}}; \overline{k_{CP}}; \overline{k_O}, \\ OCP = \langle OCP, k_{OCP}, [0; 0,2], \overline{k_{OCP}} = 0,1 \rangle, \\ CCP = \langle CCP, k_{CCP}, [0,2; 0,4], \overline{k_{CCP}} = 0,3 \rangle, \\ OP = \langle OP, k_{OP}, [0,4; 0,6], \overline{k_{OP}} = 0,5 \rangle, \\ CP = \langle CP, k_{CP}, [0,6; 0,8], \overline{k_{CP}} = 0,7 \rangle, \\ O = \langle O, k_O, [0,8; 1], \overline{k_O} = 0,9 \rangle.$ Крок 7. Розрахунок показника іншого тяжкого наслідку (ІТН): $W_{in} = \overline{W_{cc}} - k, W_{in} = W - Q \cdot k \cdot \rho = W_{cc_{\max}} - Q \cdot k \cdot \rho.$ Крок 8. Розрахунок коефіцієнта морального старіння відомостей: $K_c = 1 - T_\phi / T_n \text{ при } T_n \neq 0.$ Крок 9. Розрахунок показників економічної шкоди (ЕШ): $U_{W_{ex}} = U_{W_1} - U_{W_2}, U_{W_{in}} = U_{W_{ex}} \cdot W_{in} / W_{ex} = U_{W_{ex}} \cdot W_{in} / Q \cdot \rho \cdot k$ Крок 10. Розрахунок величини сукупної шкоди (СШ): $U_w = (\sum_{t_n=1}^{t_k} U_{W_{ex}} + \sum_{t_n=1}^{t_k} U_{W_{in}}) \cdot K_c,$ а у разі відсутності старіння цих відомостей як: $U_w = \sum_{t_n=1}^{t_k} (U_{W_{ex}} + U_{W_{in}}).$	Крок 1.5. Відомості щодо виконання секретних науково-дослідних, дослідно-конструкторських та проектних робіт, виготовлення секретних виробів. Крок 1.6. Відомості про режимні приміщення, об'єкти інформаційної діяльності. Крок 1.7. Відомості щодо факту втрати МНСІ або розголошення відомостей, що становлять ДТ, а також ІзОД іноземних держав або міжнародних організацій. <i>Етап 2. Кваліфікація порушень у сфері ОДТ.</i> Крок 2.1. Ідентифікація потенційних порушень та загроз. Крок 2.2. Ідентифікація інформації про втрату МНСІ. Крок 2.3. Ідентифікація відомостей (інформації), що становлять ДТ щодо яких відбулося порушення. <i>Етап 3. Оцінювання стану захищеності ДТ.</i> Крок 3.1. Визначення прогнозованої (бальної) величини шкоди за СС відомостей та визначення «ваги» відомостей. Крок 3.2. Визначення коефіцієнтів важливості відомостей щодо яких відбулося порушення. Крок 3.3. Визначення коефіцієнтів захищеності відомостей. Крок 3.4. Визначення переліку завдань і заходів (способів) ОДТ з усунення загроз (кіберзагроз). Крок 3.5. Визначення ефективності застосованих заходів захисту ДТ на ОКІ. Крок 3.6. Розрахунок коефіцієнту ефективності СОДТ на ОКІ. <i>Етап 4. Експертна оцінка важливості відомостей щодо яких відбулося порушення.</i> Крок 4.1. Розрахунок рівня зниження ефективності СЧО. Крок 4.2. Визначення відносної вартості СЧО. Крок 4.3. Розрахунок показника ІТН. Крок 4.4. Розрахунок коефіцієнта морального старіння відомостей. <i>Етап 5. Оцінювання негативних наслідків завданих порушенням.</i> Крок 5.1. Розрахунок показників ЕШ. Крок 5.2. Розрахунок грошової величини СШ. Крок 5.3. Розрахунок величини СШ з урахуванням територіального рівня терористичних загроз.
--	---

Висновок. Запропоновано структуру удосконалення методу аналізу і оцінювання шкоди національній безпеці України у разі витоку ДТ, яка у порівнянні від існуючого, оновлена набором ідентифікуючих та оціночних параметрів для визначення величини можливої шкоди у разі витоку ДТ у відповідності до Звіту, ЗВДТ, з урахуванням рівня терористичних загроз як для окремих тимчасово окупованих територій, так і для держави в цілому.

ЛІТЕРАТУРА

1. Про затвердження форм звітів про стан забезпечення охорони державної таємниці та інструкцій щодо порядку їх оформлення і подання, Наказ Служби безпеки України від 17.01.2020 року № 6. URL: <https://ssu.gov.ua/npb-nakazy>.
2. О. Корченко, О. Архипов, Ю. Дрейс, Оцінювання шкоди національній безпеці України у разі витоку державної таємниці: монографія, НА СБ України, Київ, 332 с., 2014.

ОСОБЛИВОСТІ ГЕОІНФОРМАЦІЙНИХ СИСТЕМ ЩО ВИКОРИСТОВУЮТЬСЯ У СУХОПУТНИХ ВІЙСЬКАХ ЗБРОЙНИХ СИЛ УКРАЇНИ

Більшість інформації у збройних силах має географічну складову (координатне прив'язування до конкретної території або до карти – розташування підрозділів, техніки, спостережних пунктів, блокпостів тощо.) Тому першочергово геоінформаційні системи (ГІС) використовувались у військах для оперативності доведення актуальної картографічної інформації одночасно до багатьох користувачів, редагування картографічної інформації та оперативно-тактичної обстановки, виконання детального аналізу місцевості, тобто для оцінки й аналізу геопросторової інформації. На сучасному етапі трансформування ЗС України ці функції ГІС значно розширились і доповнились в залежності від роду військ і способу застосування. Від початку бойових дій на сході України почала проявлятися значна прогалина у військових підрозділах – відсутність новітнього програмного забезпечення автоматизації систем управління у тактичній ланці для армії. Такий стан справ стимулював програмістів-волонтерів рухатись у напрямку створення ГІС як складової АСУ необхідних для ЗС України, щоб перемогти ворога і зберегти життя тисяч військових. Це було життєво-необхідним тому, що до прикладу, час на розрахунки для виявлення об'єкта та його знищення артилерією скорочувався в рази, не кажучи вже про точність.

Сьогодні у Збройних силах України проходять випробування, або використовуються ГІС „Арта”, навігація для військових „КомБат”, комплекс автоматизації збору і обробки розвідувальної інформації „Кропива”.

Першочергове призначення всіх систем це зменшення часу від моменту отримання даних до моменту видачі наказу підлеглим та ураження цілі, це частково виконується за рахунок заміни ланцюга голосових команд на одне повідомлення на екрані. Наступними перевагами є зменшення втрат від „дружнього” вогню унаслідок обміну інформації про положення сусідніх підрозділів, пришвидшення виходу підрозділів на бойові позиції за рахунок сучасної системи навігації, наведення вогню авіації та артилерії, попереднє планування операцій у вигляді нанесення маршрутів, розмітки зон та постановки цілей конкретним підрозділам, зменшення часу передачі координат на пункти управління та вогневі позиції, зменшення часу реагування на зміни в обстановці, зменшення своїх втрат, підвищення ймовірності ураження цілей, зменшення витрати боєприпасів. Крім цього всі три програми мають можливість взаємодії з супутниками і БпЛА і отримання від них інформації, яка в подальшому буде відображатись на карті.

Отже, головне, всі три програми створені для виконання подібних функцій, проте існують між ними певні відмінності. Так „КомБат” дозволяє здійснювати аналіз помилок після виконання операцій за рахунок модуля програвача історії подій та проводити моніторинг стану підрозділів та підлеглих. Таких функцій у інших програм немає. „Арта” та „Кропива” дозволяє негайно розраховувати установки для стрільби та передавати їх на вогневі підрозділи, виконувати вимірювання на мапі. У „Кропиві” можливе проведення топогеодезичних розрахунків. Проте не зважаючи на багато спільного, найбільшого поширення набула ГІС „Кропива”. Саме вона активно використовується тисячами військових у АТО (ООС), зберегла багато життів й є найперспективнішою, на нашу думку.

На сучасному етапі розвитку Збройних сил України під час проведення АТО (ООС) розроблено кілька систем. Дані системи були розроблені волонтерськими організаціями з залученням представників збройних сил. Недоліком є те, що жодна з цих систем не прийнята на озброєння і це не дає можливості їх використовувати у повній мірі. Дані ГІС можуть бути використані в ЗС України, якщо вони пройдуть відповідну сертифікацію та будуть прийняті на озброєння.

ВРАЗЛИВОСТІ ОПЕРАЦІЙНИХ СИСТЕМ ТА СПОСОБИ ЇХ ДЕТЕКТУВАННЯ

Актуальність дослідження. Сьогодення характеризується підвищеною увагою до проблем обробки й аналізу інформації. Невпинне зростання інформаційних масивів і кількісних даних змушує замислюватись над тим, як виконати її обробку й аналіз. Існує досить великий клас систем обробки інформації, під час розробки яких фактор безпеки відіграє першорядну роль (наприклад, банківські, медичні, економічні системи) [3, с. 11].

Одним з важливих заходів захисту інформації в комп'ютеризованих системах є визначення переліку загроз інформації. Одна або декілька загроз можуть використовувати ряд вразливостей інформації [3, с. 13]. Під інформаційною безпекою (ІБ) розуміють властивість системи протягом заданого часу протистояти несанкціонованому зняттю і модифікації інформації [2, с. 31]. Тракувати вразливість у комп'ютерній безпеці можна як неспроможність системи вчиняти супротив реалізації певної загрози чи сукупності загроз.

Постановка проблеми. Операційна система (ОС) є найважливішим програмним компонентом будь-якої обчислювальної машини, тому від рівня реалізації політики безпеки в кожній конкретній ОС залежить і загальна безпека інформаційної системи [5, с. 29]. Організація ефективного та надійного захисту ОС неможлива без превентивного аналізу можливих загроз її безпеки. Загрози безпеки ОС істотно залежать від впроваджених захисних функцій та умов експлуатації системи, від того, які процеси у ній протікають та яка інформація зберігається і обробляється в системі, тощо. Наприклад, якщо під управлінням ОС функціонує програма, що використовується для організації електронного документообігу, найбільш небезпечними загрозами є такі, що пов'язані з порушенням цілісності та доступності файлів [4, с. 3].

Загалом вразливості в ОС стають наслідком: програмних помилок (у наслідок помилки в програмному коді можна дозволити комп'ютерному вірусу отримати доступ до пристрою та взяти його під контроль); довантажених або оновлених функцій, кібератак, патчів; неправильного налаштування і адміністрування ОС [1, с. 129].

Пропонується розглянути певні нові вразливості, що виявлені у 2020 році.

Засоби безпеки ОС включають такі елементи та механізми, як облікові записи, паролі і захист файлів. Вони також включають такі менш помітні механізми, як захист ОС від ушкодження, недопущення здійснення ряду дій (наприклад, перезавантаження комп'ютера) з боку менш привілейованих користувачів і заборона несприятливої дії призначених для користувача програм на програми інших користувачів або на ОС. Таким чином, ОС, разом з окремими користувачами, має можливість захистити файли, пам'ять і налаштування конфігурації від небажаного перегляду, зміни та видалення інформації.

Але, незважаючи на існуючі засоби та механізми захисту інформації, в тому числі потужні антивірусні пакети, небезпека зараження комп'ютерів не лише не зменшується, але й продовжує зростати. Шкідливі програми свідомо і цілеспрямовано розробляються для несанкціонованого доступу, знищення, блокування, модифікації, копіювання комп'ютерної інформації або нейтралізації засобів її захисту. Перші антивірусні програми детектували дуже мало вірусів, це були одиниці чи десятки загроз. Ви могли завантажити антивірус, який був здатний виявити лише 30 загроз, і це було нормально. Звісно, почали з'являтися багато маленьких антивірусів, які детектували не багато, але різних вірусів. Далі антивіруси почали розвиватись разом з ОС та технологічною частиною комп'ютерів. Із самого початку появи антивірусних програм, програмісти зрозуміли, що вірус потрібно детектувати за певною характеристикою. Кожен антивірус містить мінімальний базовий набір технологій: сигнатурний аналізатор, евристичний аналізатор, поведінковий аналізатор, набір фільтрів, перехоплення подій файлової системи, електронної пошти, можливо і інших каналів. Також

набір інструментів, які дозволяють користувачу увімкнути / вимкнути захист у режимі реального часу, провести вибіркове сканування і виконати дії над знайденими вірусами. Крім цього існують продукти, які виходять за межі функціонування безпосередньо антивірусних програм, створюючи нові класи продуктів ІБ. Це програми класу Internet Security, Total Security, Mega Security. Ще один важливий момент – захист комп'ютера від вірусів проводиться не лише за рахунок антивірусу. Нажаль, антивірус не є повною панацеєю від вірусів. Він може заблокувати 99% загроз чи навіть 99,9 %, але ж не 100 %!

Так, Microsoft Corporation 14.01.2020 року випустила виправлення програмного забезпечення для захисту 49 вразливих місць у рамках щомісячного оголошення Patch Tuesday. Серед виправлених вразливостей були критичні недоліки в Windows Crypto API, шлюз віддаленого робочого столу Windows (RD Gateway) та клієнт віддаленого робочого столу Windows. Зловмисник може віддалено використовувати ці вразливості для дешифрування, зміни або введення даних на з'єднання користувачів. Вразливість підробки Crypto API (CVE-2020-060). Ця вразливість впливає на всі робочі станції, на яких працює 32-або 64-розрядні операційні системи Windows 10, включаючи версії Windows Server 2016 і 2019 [1, с. 130]. Даний тип вразливості дозволяє зловмисникам перевірити сертифікат криптовалюту Elliptic Curve, щоб обійти довіру, дозволяючи шкідливому програмному забезпеченню ховатись під автентичне підписання надійною, довіреною організацією. Це надає можливість перешкоджати виявленню зловмисних програм. Як варіант, може бути створений зловмисний сертифікат для імені хоста, яке його не авторизувало. У такому разі, браузер, який перекидає роботу на Windows Crypto API, не покаже попередження і дозволить зловмиснику дешифрувати, змінити або ввести дані для з'єднання користувачів без їх виявлення. Вразливості клієнта шлюзу Windows RD та віддаленого робочого столу Windows (CVE-2020-0609, CVE-2020-0610 та CVE-2020-0611). Вони актуальні для Windows Server 2012 та Windows 7 і новіших. Ці вразливості – на клієнтах віддаленого робочого столу Windows та на сервері шлюзу RD – дозволяють виконувати віддалене виконання коду. Вразливості сервера не потребують автентифікації чи взаємодії з користувачем, і їх можна експлуатувати спеціально створеним запитом. Вразливість клієнта можна використати, переконавши користувача підключитися до шкідливого сервера [1, с. 132].

Висновок. Отже, за допомогою ОС комп'ютер, здатний виконувати лише дії, які визначаються системою команд, перетворюється у віртуальну машину, що виконує широкий набір набагато складніших функцій. Виникнення потенційних загроз безпеки пов'язано з наявністю вразливостей. Вразливість – це недолік або слабе місце, яке може бути використане для реалізації загрози. Виділивши окремо найбільш важливі елементи ОС, можливо досягти повноцінного захисту системи із повноцінним захистом, найбільш наближеним до ідеального.

ЛІТЕРАТУРА

1. Ільєнко А. В. Перспективні методи захисту операційної системи Windows / А. В. Ільєнко, С. С. Ільєнко, Т. М. Куліш // Кібербезпека: освіта, наука, техніка. – 2020. – № 4. – С. 124 – 134.
2. Козачок В. А. Технології протидії шкідливим програмам та завідома фальшивому програмному забезпеченню / В. А. Козачок, А. А. Рой, Л. В. Бурячок // Сучасний захист інформації. – 2017. – № 2. – С. 30 – 34.
3. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. 3–38 Захист інформації в комп'ютерних системах: підручник. – Ніжин: ФОП Лук'яненко В.В., ТПК „Орхідея”, 2020. – 236с.
4. Лозинський Д.Н. Інформаційна безпека. Проблема нового тисячоліття / Д. Н. Лозинський, Е. В. Плєскач // Системи безпеки. – 2014. – № 4(46). – С. 13.
5. Розподілений антивірусний контроль як спосіб протидії зловмисним програмами в автоматизованих інформаційних системах / С.В. Скриль та ін // Радіосистеми. – Вип. 37 „Радіотехнічні та інформаційні системи охорони і безпеки”. – Радіотехніка. – 2014. – №6. – С. 27 – 30.

МОДЕЛЬ УПРАВЛІННЯ ТА РОЗПОДІЛУ ТРАФІКУ В РАДІОМЕРЕЖАХ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ

При переході від комутації каналів до комутації пакетів відбувається зміна структури і інтенсивності трафіку. У мережах з комутацією каналів прийнято використовувати Марковські моделі, за допомогою яких можна обчислити вірогідність втрат викликів при обраної ємності каналів і забезпечити необхідну якість обслуговування. У разі мереж з комутацією пакетів, до яких відносяться радіомережі тактичної ланки управління (РМ ТЛУ), необхідно вирішувати завдання, пов'язані із затримками пакетів, ймовірністю їх втрат і ефективним використанням пропускнуєї спроможності. На сьогоднішній день велика кількість відомих вчених, наприклад, Kleinrock, S. Blake, D. Grossman, Z. Wang, Стеглов В.К., Беркман Л.Н., а також дослідницькі центри, такі як Mobile Ad-hoc Networks, Center for Embedded Networked Sensing займаються питаннями управління і розподілу трафіку. Однак, незважаючи на величезну кількість публікацій, завдання побудови моделей управління трафіком, які найкращим чином відображають його функціонування в реальних умовах, все ще не вирішена. Абоненти РМ ТЛУ повинні мати можливість передавати по мережі різні види пакетного трафіку. Інформаційні повідомлення радіомережі, утворюють мультимедійний трафік (мовні повідомлення, відео) і трафік даних (сигнали управління, текстові повідомлення, топографічні зображення, інша інформація). Для якісної передачі потокового трафіку необхідно мінімізувати затримку пакетів і її дисперсію, при цьому допускаються незначні втрати пакетів. При передачі даних, навпаки, затримки окремих пакетів на якість передачі даних не впливають, але при цьому потрібна гарантована доставка кожного пакета. Зазначені процедури істотно ускладнюють процес передачі даних і збільшують час доставки повідомлень. Для обґрунтування оптимальних і дієвих інструментів моделювання процесів управління і розподілу трафіку детально проаналізовані проблеми, що виникають в процесі роботи бездротових мереж, що призводять до затримки передачі бітів. Існуючі засоби моделювання бездротових мереж відображають лише окремі параметри трафіку і не забезпечують його ефективне управління і розподіл. Отже, в даний час виникає потреба в нових моделях управління і розподілу трафіку в бездротових мережах, які здатні будуть забезпечити високу якість обслуговування з урахуванням різних вимог, що обумовлює актуальність і практичну значущість обраної теми дослідження.

В процесі моделювання трафіку бездротової мережі доцільно здійснювати конфігурацію кластерів, що дозволить зменшити час на передачу інформації і оптимізувати мережевий трафік. Тому, для критерію вибору структури і розміру кластерів слід визначити ефективність передачі даних. Критерієм ефективності управління і розподілу трафіку є службовий трафік, який повинен бути зведений до мінімуму. Обсяг службового трафіка залежить від частоти реконфігурацій мережі і кількості кластерів в мережі. У той же час незалежно від того, який саме математичний інструментарій буде обраний для управління і розподілу трафіку в бездротових мережах необхідно проводити верифікацію отриманої моделі.

Висновки. З метою вибору оптимального і результативного математичного апарату моделювання розподілу і управління трафіком в бездротових мережах проаналізовані проблеми, що викликають затримку передачі бітів. На підставі отриманих результатів обґрунтовано необхідність і доцільність використання алгоритмів управління чергами та методів реконфігурації кластерів. Для проведення верифікації отриманих моделей запропоновано використовувати критерії адекватності моделі еталонного трафіку. Таким чином, представлено вирішення актуальної науково-технічної задачі, що складається в розробці імітаційної моделі управління інформаційними потоками в РМ ТЛУ. Модель повинна враховувати основні особливості передачі потоків даних і реального часу у мережі, що функціонує в умовах динамічної топології і деструктивних зовнішніх впливів.

АНАЛІЗ МОДЕЛЕЙ ЖИВУЧОСТІ ЯК ВЛАСТИВОСТІ СИСТЕМИ ЗВ'ЯЗКУ

Аналіз публікацій з питань дослідження живучості систем зв'язку військового призначення показує, що вона визначає працездатність системи зв'язку в певних умовах експлуатації, проте методи аналізу і забезпечення показників живучості суттєво відрізняються.

Слід звернути увагу на те, що, на сьогодні не існує розвиненої теорії, яка б дозволяла досліджувати живучість як властивість системи зв'язку, оцінювати її кількісно, розробляти практичні рекомендації щодо забезпечення живучості.

Під живучістю розуміємо здатність системи зв'язку до збереження основних функцій при впливі несприятливих факторів (зовнішнього середовища або впливу супротивника), які виходять за рамки проектних умов експлуатації.

Іншими словами, живучість – це властивість об'єкту, яка полягає в його здатності виконувати завдання за цільовим призначенням в процесі несприятливих впливів (НВ) на весь об'єкт або окремі його елементи, підтримуючи в допустимих межах основні експлуатаційні показники.

Для практичного застосування найбільш придатні імовірнісні та детерміновані моделі.

Імовірнісні моделі будуються з припущенням про рівномірний закон розподілу НВ в об'ємі досліджуваної системи зв'язку або з припущенням про однаковий об'єм руйнувань, які виникають в будь-якому місці системи зв'язку при реалізації одноразового (однократного) НВ.

Детерміновані моделі живучості будуються на основі зіставлення конкретних видів вражаючих факторів НВ і стійкості до них елементів та об'єкту дослідження в цілому. У цьому напрямі виділяють два підходи: статичний і динамічний.

Важливі переваги динамічного підходу полягають в урахуванні фактора часу при визначенні рівня працездатності об'єкту дослідження і можливості отримання кількісних залежностей показників живучості від значення параметрів об'єкту.

В даний час проблемним є формування показників живучості для детермінованого динамічного підходу. Області працездатності можуть бути побудовані як в просторі параметрів об'єкта, так і в просторі параметрів НВ.

У першому випадку в якості показників живучості приймаються параметри об'єкту дослідження, а їх критичні значення (відповідні межі непрацездатності об'єкта) виступають як кількісні оцінки живучості.

У другому випадку показники – це параметри НВ, кількісні оцінки яких є значеннями параметрів НВ, при яких система переходить в область непрацездатності. Подвійність у виборі показників живучості, з одного боку, дозволяє сформулювати вимоги до параметрів системи і її структури, включаючи топологічну структуру, з іншого боку – отримати вимоги для розробки і застосування заходів або засобів протидії НВ.

З аналізу визначення живучості та порівняння методів і моделей, які застосовуються для їх оцінки, випливають основні проблеми їх дослідження:

- вибір рівня декомпозиції об'єкту дослідження;
- вибір моделі відмов елементів системи зв'язку (тип моделі, математичний апарат);
- вибір показників ефективності;
- вибір методу знаходження кількісних значень показників;
- вибір початкових вихідних даних;
- вибір способів забезпечення живучості (працездатності системи зв'язку).

Живучість визначається як зовнішньою, так і внутрішньою властивостями системи зв'язку. Для систем зв'язку військового призначення живучість доцільно розглядати як внутрішню властивість системи, яка досягається шляхом здійснення ряду організаційних та технічних заходів.

ПЕРСПЕКТИВИ ЗБЕРЕЖЕННЯ СТІЙКОСТІ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ТА ПОБУДОВАНИХ НА ЇХ ОСНОВІ СИСТЕМ ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ В УМОВАХ СТІМКОГО РОЗВИТКУ КВАНТОВИХ КОМП'ЮТЕРІВ

Актуальність. В умовах постійної модернізації засобів автоматизованої обробки даних та їх програмного забезпечення необхідно постійно вдосконалювати системи закриття інформації (даних). Криптографічна стійкість (або крипостійкість) – здатність криптографічного алгоритму протистояти криптоаналізу. Стійким вважається алгоритм, який для успішної атаки вимагає від противника недосяжних обчислювальних ресурсів, недосяжного обсягу перехоплених відкритих і зашифрованих повідомлень чи ж такого часу розкриття, що по його закінченню захищена інформація буде вже не актуальна, і т. н.

Модернізація засобів автоматизованої обробки даних як раз й наближає вказану недосяжність обчислювальних ресурсів до реальних показників „досяжності”. Так, наприклад компанія D-Wave Systems, у 2007 році продемонструвала 16-кубітний комп'ютер Orion, а в листопаді того ж року – 28-кубітний комп'ютер. Інша компанія - IBM представила в березні 2018-го року 72-кубітний квантовий комп'ютер Google Bristlecone.

Постановка задачі. В залежності від складності злому алгоритми шифрування забезпечують різні ступені захисту, відповідно, передбачаючи цілі і можливості криптоаналітика необхідно змінювати і стійкість ключа з метою надійного захисту інформації.

Мета. Дослідити перспективи збереження стійкості існуючих криптоалгоритмів та систем з огляду на перспективи зростання потужностей обчислювальних засобів.

Основні положення. В залежності від складності злому, алгоритми забезпечують різні ступені захисту.

Під час розгляду загроз на перше місце ставиться принципова можливість отримання за допомогою перехоплення інформації про відкритий текст або використані ключі.

На другому місці розглядається можливість зламу системи закриття інформації шляхом криптоаналізу (повним перебором всіх ключів, та (або) розкриття криптографічного алгоритму) за рахунок збору необхідного обсягу перехоплених відкритих і зашифрованих повідомлень.

Відповідно до застосованих криптоалгоритмів розглядають три типи криптостійких систем шифрування:

Абсолютно стійкі системи – системи створенні на основі абсолютно стійких алгоритмів шифрування (були визначені Клодом Шенноном і опубліковані в роботі „Теорія зв'язку в секретних системах”). Там же визначено вимоги до такого роду систем:

ключ генерується для кожного повідомлення (кожен ключ використовується один раз);

ключ статистично надійний (тобто ймовірності появи кожного з можливих символів рівні, символи в ключовий послідовності незалежні і випадкові);

довжина ключа дорівнює або більше довжини повідомлення;

вихідний (відкритий) текст має деяку надмірність (є критерієм оцінки правильності розшифрування).

Стійкість цих систем не залежить від того, якими обчислювальними можливостями володіє криптоаналітик. Практичне застосування систем, що задовольняють вимогам абсолютної стійкості, обмежене міркуваннями вартості і зручності користування.

Доказово стійкі (практично стійкі) системи – системи засновані на основі криптоалгоритмів стійкість яких доказово визначається складністю рішення добре відомої математичної задачі, яку намагалися вирішити багато математиків і яка є загальновизнано складною. Як приклад, можна привести системи DH (Діффі-Хеллмана) і RSA (Ривеста-

Шаміра-Адельмана), засновані на складності дискретного логарифмування і розкладання цілого числа на множники відповідно.

Імовірно стійкі системи – системи засновані на основі імовірно стійких криптоалгоритмів, які базуються на складності рішення приватної математичної задачі, яка не зводиться до добре відомих завдань, і яку намагалися вирішити одна або кілька осіб. Прикладами можуть служити шифри ГОСТ 28147-89, AES, FEAL.

В основному застосовуються практично стійкі (доказово стійкі) або обчислювально стійкі (ймовірно стійкі) системи. Стійкість цих систем залежить від того, якими обчислювальними можливостями володіє криптоаналітик. Практична стійкість таких систем базується на теорії складності і оцінюється виключно на якийсь певний момент часу і послідовно с двох позицій:

обчислювальна складність повного перебору;

відомі на даний момент слабкості (уразливості) та їх вплив на обчислювальну складність.

У кожному конкретному випадку можуть існувати додаткові критерії оцінки стійкості.

Оцінка криптостійкості систем шифрування як правило проводиться двома етапами:

Початкова оцінка: оскільки атака методом грубої сили (повним перебором всіх ключів) можлива для всіх типів криптографічних алгоритмів, крім абсолютно стійких „по Шеннону”, для новоствореного алгоритму вона може бути єдиною існуючою. Способи її оцінки ґрунтуються на обчислювальній складності, яка потім може бути виражена у часу, грошах, і необхідній продуктивності обчислювальних ресурсів, наприклад, в MIPS. Ця оцінка поки є максимальною і мінімальною одночасно.

Поточна оцінка: подальше дослідження алгоритму з метою пошуку слабкостей (вразливостей) (криптоаналіз) додає оцінки стійкості по відношенню до відомих криптографічних атак (лінійний криптоаналіз, диференціальний криптоаналіз і більш специфічні) і можуть знизити відому стійкість.

Наприклад, для багатьох симетричних шифрів існують слабкі ключі та S-блоки, застосування яких знижує криптографічну стійкість. Також важливим способом перевірки стійкості є атаки на реалізацію, що виконуються для конкретного програмно-апаратно-людського комплексу.

Чим більш тривалим і експертним є аналіз алгоритму і реалізацій, тим більше достовірної можна вважати його стійкість. У кількох випадках тривалий і уважний аналіз приводив до зниження оцінки стійкості нижче прийнятного рівня (наприклад, в чорнових версіях FEAL). Недостатня перевірка (на думку багатьох криптографів – штучне ослаблення) алгоритму потокового шифрування A5/1 привела до успішної атаки.

Як що проаналізувати зростання продуктивності обчислювальних ресурсів можна побачити зниження обчислювальній складності, яка може бути виражена у часі який необхідно витратити на атаку методом грубої сили (повним перебором всіх ключів).

В публікаціях Національної академії наук США (National Academy of Sciences) наводяться приблизні розрахункові терміни зламу існуючих криптоалгоритмів. Де-які з них можуть бути зламані на протязі реального часу (RSA з довжиною ключа 80-128 біт викривається протягом 6-229 годин, ECC з довжиною ключа 256-512 біт викривається протягом 10-95 годин), інші мають більш надійну стійкість (на злам AES-GCM необхідно як мінімум 2.61×10^{12} років, SHA256 (Bitcoin mining) – мінімум 1.8×10^4 років).

Але всі ці прогнози були зроблені станом на 2018 рік, а вже в 2019 році команда вчених з університету Нового Південного Уельсу створила найбільш швидкі в світі двокубітні вентиля на атомах кремнію. Вчені повідомляють, що їм вдалося створити пристрій яких виконує розрахункову операцію всього за 0,8 нс. Це приблизно в 200 раз швидше існуючих аналогів.

Висновок. Зважаючи на постійне зростання продуктивності обчислювальних ресурсів необхідно шукати нові методи створення доказово стійких (практично стійких) систем з наближенням їх до абсолютно стійких систем. В противному випадку надійність закриття інформації буде неухильно знижатися, що обов'язково в підсумку приведе до негативних наслідків.

АНАЛІЗ НЕОБХІДНОСТІ ЗАСТОСУВАННЯ ЦЕНТРІВ СЕРТИФІКАЦІЇ У МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Актуальність обраної теми зумовлена тим, що сьогодні в умовах збройної агресії з боку Російської федерації та ведення війни на території нашої країни питання безпеки державних інформаційних ресурсів, зокрема Збройних Сил України, є пріоритетним. Сьогодні більшість інформаційних ресурсів спеціального призначення використовують придбані сертифікати зарубіжних компаній терміном 1-5 років, що являє собою не раціональним використанням коштів (вартість 1 доменного сертифікату на рік становить 500\$), або взагалі працюють без них (рис.1). Створення власного центру сертифікації (ЦС) ЗСУ відкриє можливості економії фінансових ресурсів а також забезпечить реалізацію та функціонування власної інфраструктури відкритих ключів для безпечної передачі важливих даних для навігації, отримання пошти, спілкування, обміну файлами, блокуючи можливість атаки “man in the middle”, а також створення дублікату сайту.

Мета дослідження полягає у обґрунтуванні необхідності проектування та створення інфраструктури відкритих ключів, аналізі можливостей та реальних перспектив використання власних центрів сертифікації в інтересах ЗСУ, для підвищення безпеки інформаційних ресурсів спеціального призначення.

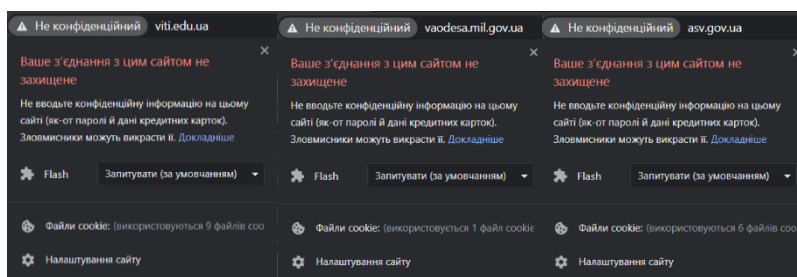


Рисунок 1. Відсутність захисту інформаційних ресурсів ЗСУ

Виклад основного матеріалу. Розробка тривірневої ієрархії PKI (Public Key Infrastructure) (рис.2) яка включає один центр сертифікації ключів та кілька проміжних центрів забезпечить реалізацію власної інфраструктури відкритих ключів. Кореневий ЦС випускає сертифікати тільки для проміжних ЦС, а вже проміжний ЦС забезпечує видачу сертифікатів кінцевим споживачам.

Одноразове розгортання та довгий час дії кореневого ЦС дозволяє ізолювати його від мережі. Це автоматично зводить до нуля можливість компрометації такого ЦС, оскільки без доступу до мережі до нього не дістанися.

Висновки. Виконане дослідження загальних можливостей та перспектив застосування центру сертифікації в інтересах Збройних Сил України показало необхідність створення центру сертифікації ЗСУ. В ході подальших досліджень планується розробити інфраструктуру центрів сертифікації які б підвищили безпеку інформаційних ресурсів спеціального призначення.

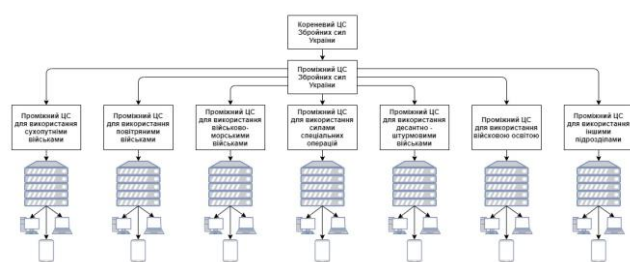


Рис. 2. Схема ієрархії Public Key Infrastructure

ЗАХОДИ ДЛЯ БЛОКУВАННЯ ДІЇ ВІРУСУ ШИФРУВАЛЬНИКА В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ

Постановка завдання. В тезах запропонована послідовність дій адміністратора системи для протидії спробам несанкціонованого шифрування інформації в інформаційно-телекомунікаційній системі в умовах кібератаки шкідливим програмним забезпеченням типу вірус шифрувальник.

На актуальність розробки таких заходів вказують висновки найкращих світових кіберфахівців, які вказують, що кількість атак вірусу шифрувальника досягає до 30 відсотків від загальної кількості інцидентів у світі. Масовані атаки відбуваються кожного півроку, а техніки проникнення до інформаційно-телекомунікаційної системи та шифрування значно покращуються. Згідно моделі Cyber-Kill Chain зловмисники вдало досягають встановленої мети на цільовій машині в визначеній мережі.

Мета доповіді. Метою заходів для нейтралізації несанкціонованого шифрування інформації в інформаційно-телекомунікаційній системі є повне унеможливлення початку роботи вірусу шифрувальника або блокування його дії на самому початку роботи.

Автори пропонують завчасно розгортати в інформаційно-телекомунікаційній системі зразки спеціального програмного забезпечення, які дозволять своєчасно виявляти ознаки підготовки та початок несанкціонованого шифрування інформації, оперативне блокувати шифрування, робити аварійне копіювання важливої інформації що циркулює в інформаційно-телекомунікаційній системі, а при необхідності відновити зашифровану інформацію за рахунок оперативного виявлення ключової інформації та відновити процес штатного функціонування інформаційно-телекомунікаційної системи.

Виклад основного матеріалу. Заходи передбачають завчасне розміщення в інформаційно-телекомунікаційній системі зразків спеціального забезпечення, які здатні реалізувати програмне чергування за процесами в інформаційно-телекомунікаційній системі, здійснення програмно керованої зупинки процесора інформаційно-телекомунікаційної системи при виявленні ознак шифрування, а саме: при спробі перевантаження цільової машини, при виявленні підозрілих процесів, при виявленні ознак дії алгоритму шифрування, при синхронному зникненні важливих файлів та появі нових шифрованих файлів, та ін.. Автори вважають, що призупинення роботи процесора дасть можливість вчасно зупинити процес шифрування, надасть можливість адміністратору інформаційно-телекомунікаційної системи здійснити ефективний аналіз ознак шифрування, здійснити оповіщення про загрозу, здійснити аварійне копіювання інформації, здійснити пошук ключів, забезпечити пошук тіла шифрувальника, а також при необхідності здійснити відновлення знищених або зашифрованих файлів та остаточно відновити роботу інформаційно-телекомунікаційної системи згідно її функціоналу. Автори порівнюють кіберзахищеність інформаційно-телекомунікаційної системи без застосування запропонованих заходів захисту інформаційно-телекомунікаційної системи від шифрування та з ними. Автори вважають, що кіберзахищеність інформаційно-телекомунікаційної системи від шифрування зростає до 0,99 в залежності від ефективності заходів та якості обізнаності адміністраторів та користувачів.

Висновки. Висновками тез є те, що завчасна розробка та розміщення спеціалізованих програмних засобів в інформаційно-телекомунікаційній системі дозволить своєчасно втрутитись в дії вірусу шифрувальника та підвищити захищеність інформаційно-телекомунікаційної системи від дій вірусу шифрувальника до задовільного рівня.

Подальші напрямки досліджень дозволять запропоновані заходи поширити для нейтралізації дій різних класів шкідливого програмного забезпечення – руткітів, хробаків, бекдорів та вірусів, враховуючи при цьому специфіку їх діяльності.

Ключові слова: вірус-шифрувальник, методика, показник, сервіс, кібератака, кіберзачишувач, кіберзахищеність, інформаційно-телекомунікаційна система.

ПІДХІД ДО КЛАСИФІКАЦІЇ ЗАГРОЗ ІНФОРМАЦІЇ НА ОБ'ЄКТИ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Інформаційна безпека (ІБ) є важливою складовою національної безпеки держави в цілому. Захищеність інформації об'єктів критичної інфраструктури, в тому числі і об'єктів інформаційної діяльності (ОІД), безпосередньо впливає на стан ІБ держави. Визначення рівня захищеності інформації пов'язано з загрозами, які безпосередньо можуть впливати на конфіденційність, цілісність та доступність інформації. Оскільки інформація для суспільства займає одну з найважливіших позицій, то й відповідно вимоги до її захисту потребують удосконалення, з метою проведення оцінювання рівня ІБ ОІД та створення ефективних і перспективних систем захищеності інформації на ОІД. Особливо вирішення такого наукового завдання стає актуальним в умовах збройної агресії Російської Федерації проти України та постійного впливу на всі сфери діяльності суспільства. Разом з тим необхідність додаткового дослідження можливих загроз інформації ОІД покликане реформуванням системи охорони державної таємниці з урахуванням практики держав-членів Організації Північноатлантичного договору та Європейського Союзу. Доцільно проводити дослідження щодо розроблення нових підходів та удосконалення існуючих класифікаторів загроз інформації оскільки з розвитком інформаційних технологій зростає й рівень небезпеки, що може в свою чергу впливати на функціонування інформаційно-телекомунікаційних систем та ОІД. Підходи до класифікації загроз інформації висвітлені у багатьох публікаціях, як вітчизняних так і закордонних вчених. Також створена нормативно-правова база України в галузі технічного захисту інформації, яка дозволяє класифікувати загрози інформації за певними ознаками. Впровадження досвіду країн НАТО під час створення комплексів технічного захисту інформації та комплексних систем захисту інформації на ОІД потребує систематизації загроз інформації за визначеними ознаками та їх представлення у вигляді універсальної системи для користування. В той же час питанню класифікації загроз інформації за визначеними ознаками приділено недостатньо уваги, що призводить до упущень, і як наслідок створення неефективних систем захисту інформації. На основі аналізу нормативно-правових документів можна зробити висновок, що на даний час до кінця не сформований чіткий механізм (алгоритм) визначення загроз для інформації об'єкту критичної інфраструктури. У результаті проведеного аналізу можливих загроз інформації на ОІД, які регламентуються нормативно-правовими документами в галузі технічного захисту інформації, сформовано мету наукового дослідження, яка полягає в удосконаленні підходів до класифікації загроз інформації на ОІД. Досягнення поставленої мети реалізовано за рахунок обраних загроз інформації за визначеними ознаками. Запропонована фасетна класифікація загроз інформації на ОІД враховує такі складові, як джерело загрози, канал поширення загрози, метод реалізації загрози та можливі наслідки від їх реалізації. Даний класифікатор дозволяє формувати код загрози за обраними ознаками та визначати уразливість системи захисту інформації, що дає можливість систематизації та синтезу моделі загроз інформації та моделі порушника. Також відповідно формалізованого класифікатора запропоновано організаційні та інженерно-технічні заходи, які комплексно можливо застосовувати для протидії загрозам інформації на ОІД. Розроблений фасетний класифікатор загроз дозволяє додавати нові ознаки класифікації без зміни загальної структури, що дозволяє більш ефективно оцінити рівень загрози інформації на ОІД.

Запропонований підхід до класифікації загроз інформації об'єктам критичної інфраструктури дасть змогу більш об'єктивно визначати необхідні заходи щодо організації та створення комплексів технічного захисту інформації (комплексних систем захисту інформації).

Лазута Р.Р. (ВІТІ)
Прис Г.П. (ВІТІ)
Троцько Л.Г. (ВІТІ)
Макогон О.А. (ВІТВ НТУ „ХПР”)

АНАЛІЗ УМОВ ДЛЯ ВПРОВАДЖЕННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СТАНДАРТІВ НАТО В ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Забезпечення якісними системами телекомунікації підрозділів Збройних Сил України сьогодні є одним із найважливіших завдань, які стоять в контексті їх системного реформування. Одним із ключових питань, яке необхідно вирішувати в сучасних умовах – яким чином і коли здійснювати перехід на стандарти НАТО, не втрачаючи при цьому необхідного рівня функціонування систем зв'язку та передачі даних. Такий перехід необхідно здійснювати, враховуючи наявні можливості та ресурси, які виділяються для реформування Сектору безпеки і оборони України. Запровадження в ЗС України натівських систем зв'язку не є простою заміною технічних засобів, які б відповідали стандартам НАТО або переведенням на нові нормативи використання, це складне комплексне завдання, що вимагає поєднання, організаційних зусиль, технічних напрацювань, певної зміни способів управління та взаємодії. В цьому контексті актуалізується питання стосовно термінів переведення систем телекомунікації ЗС України на стандарти НАТО. Дослідження цього питання і отримання відповіді на нього дасть змогу забезпечити планування заходів з переходу на стандарти НАТО без втрати ефективності вже існуючих систем телекомунікації. Конкретне питання – впровадження телекомунікаційних стандартів НАТО та термінів досяжності сумісності в цій сфері з державами-членами альянсу розглянуто не було.

Впровадження телекомунікаційних стандартів НАТО в ЗС України – процес, що передбачає введення спільного порядку дій, закріплення єдиної термінології і встановлення умов уніфікації технічних процесів в системах телекомунікації і зв'язку ЗС України та країн НАТО, а також країн-партнерів. Стандарти НАТО в сфері телекомунікації, за аналогією, можна розділити на адміністративні, оперативні та матеріально-технічні:

адміністративні стандарти визначають процеси управління та обміну інформацією, порядок роботи з документацією;

стандарти спрямовані на оперативне планування застосування систем телекомунікації та зв'язку;

матеріально-технічні стандарти визначають єдині вимоги до озброєння і військової техніки союзників, управлінню життєвим циклом, а також кодифікації предметів забезпечення в сфері телекомунікації.

В основу аналізу умов для впровадження телекомунікаційних стандартів НАТО в Збройних Силах України був покладений аналітичний метод (ANP-process) який передбачає врахування часових умов, ресурсних можливостей та особливості технічних рішень. В результаті аналізу виявлено, що повноцінно впровадити стандарти НАТО в телекомунікаційній сфері можливо лише у довгостроковій перспективі (12 років і більше). Це пов'язано, в першу чергу, з рядом умов, виконання яких в короткостроковій та середньостроковій перспективі неможливе. До цих умов належать фінансові та організаційно-технічні. Це підтверджується зокрема тим фактом, що повноцінне впровадження телекомунікаційних стандартів НАТО в Збройних Силах України розпочалося наприкінці 2015 року, а імплементація з 2016 року, з того часу суттєвих зрушень, що могли б свідчити про інтенсифікацію цього процесу не відбулося. Сьогодні очевидно, що для ефективного запровадження цих стандартів, очевидно, потрібен комплекс додаткових заходів. До цих заходів відносяться здійснення ефективного планування процесу впровадження, створення тимчасових структур, відповідальних за запровадження стандартів НАТО та посилення взаємодії з представниками НАТО в Україні.

МЕТОД ОБРОБКИ ВІДЕОІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Актуальність. Розвиток комп'ютерних систем та мереж визначається трьома факторами: ростом трафіку, потребою суспільства в нових послугах та досягненнями в області технологій. Зрозуміло, ці фактори не є незалежними, проте кожен з них визначає ідеологію розвитку комп'ютерних мереж. Удосконалення програмно-апаратних компонентів обробки відеоінформації в комп'ютерних системах та мережах спеціального призначення, які визначаються зростанням обсягів трафіку та потребою суспільства в появі сучасних послуг, призводять до необхідності постійного збільшення та модернізації комп'ютерних систем та мереж спеціального призначення. Існуючі механізми забезпечують вплив на інтенсивність потоку відеоінформації за рахунок непередбачених втрат інформації та значних затримок на обробку. Отже, необхідно дослідити умови і причини виникнення підвищеної інтенсивності відеопотоку.

За основні критерії класифікації трафіку прийняті три характеристики: відносна передбачуваність швидкості передачі даних, чутливість трафіку до затримок пакетів і чутливість трафіку до втрат і спотворень пакетів.

Постановка задачі. Комп'ютерні системи та мережі спеціального призначення – це інтегрований комплекс організаційних, технічних заходів та взаємозв'язаних і погоджено-функціонуючих програмних та програмно-апаратних компонентів, що забезпечують достовірну обробку, збереження та передачу інформації від джерела повідомлення до споживача з урахуванням особливостей силових та спеціальних структур України.

Метою доповіді є розробка методу обробки відеоінформації в комп'ютерних системах та мережах спеціального призначення з врахуванням вказаних особливостей.

Основні положення. Існуючі механізми забезпечують вплив на інтенсивність потоку відеоінформації за рахунок непередбачених втрат інформації та значних затримок на обробку. Розвиток програмно-апаратних компонентів обробки відеоінформації в комп'ютерних системах та мережах спеціального призначення, які визначаються зростанням обсягів трафіку та потребою суспільства в появі сучасних послуг, призводять до необхідності постійного зростання і модернізації комп'ютерних систем та мереж. Найбільш популярними останнім часом стають відеоінформаційні послуги. Проблемними особливостями надання відеоінформаційних послуг в комп'ютерних системах та мережах спеціального призначення є: висока інтенсивність відеопотоку; нерівномірність відеопотоку за часом; чутливість до затримок та втрат пакетів при передачі.

Отже, підвищення якості відеоінформаційного сервісу в комп'ютерних системах та мережах спеціального призначення є актуальною науково-прикладною проблемою. Одним з ефективних напрямків підвищення продуктивності комп'ютерних систем та мереж спеціального призначення є зниження інтенсивності вхідного відеопотоку на основі його компресії. У цьому випадку знижується завантаження вузлів комутації, час затримки та ймовірності втрати пакетів на вузлах комп'ютерних систем та мережах спеціального призначення. Тому при формуванні відеотрафіка в першу чергу необхідно контролювати відповідність бітової швидкості джерела відносно пропускну здатності каналів зв'язку.

Висновок. Запропонований метод дозволяє вдосконалити програмно-апаратні компоненти обробки відеоінформації в комп'ютерних системах та мережах спеціального призначення, який дозволяє побудувати систему управління бітової швидкістю відеопотоку в комп'ютерних системах та мережах з низькою пропускну здатністю каналу.

ВДОСКОНАЛЕННЯ СИСТЕМИ РАДІОЧАСТОТНОЇ ІДЕНТИФІКАЦІЇ В ТЕХНОЛОГІЇ ДОПОВНЕНОЇ РЕАЛЬНОСТІ

Аналіз існуючих і перспективних систем управління бойовими діями Збройних Сил розвинених держав світу передбачає високий рівень оснащення військ новітніми, у т.ч. автоматизованими і роботизованими видами ОВТ, а також системами, засновані на нових фізичних принципах, що у свою чергу впливає на розвиток сучасного поля бою і вимагає вживати відповідних заходів, для створення нових систем і засобів протидії.

До теперішнього часу в Збройних Силах держав світу створені робототехнічні комплекси військового призначення, оснащені перспективними засобами спостереження, що забезпечують автономне ведення розвідки і видачу даних оператору за допомогою системи доповненої реальності. Для того, щоб додаток доповненої реальності швидко розпізнав об'єкт, на ньому розміщується маркер. В якості маркерів використовуються мітки системи радіочастотної ідентифікації (RFID), які не вимагають аналізу великого обсягу даних.

Однак, в залежності від цільового призначення системи RFID необхідно враховувати спосіб її реалізації, тип даних, пристрої доповненої реальності, об'єм даних, вимог до мережі передачі даних, вимоги до серверного обладнання, способу ідентифікації об'єктів, що набуває особливої актуальності останнім часом. Системи RFID функціонують на основі колективного використання частот і уніфікації сигналів різноманітних радіоелектронних засобів. При цьому основним критичним компонентом у цифрових модемах, які забезпечують точну синхронізацію фаз, крок, точність налаштування і час перебудови за частотою, є синтезатор частоти (СЧ), побудований за схемою фазового автопідстроювання частоти (ФАПЧ). Цим вимогам частково задовольняють цифрові системи ФАПЧ, час перебудови яких залежить від дискримінаційної характеристики фазового детектора і динамічних властивостей петлі ФАПЧ, зміна яких прискорює пошук і захоплення частоти і фази та призводить до погіршення спектральних характеристик генерованого колювання. Є велика кількість рішень, що покращують динамічні характеристики ФАПЧ за рахунок оптимізації дискримінаційної характеристики фазового детектора, та зміни смуги пропускання фільтра нижніх частот, шляхом зміни його структури в перехідному режимі.

Проте основним недоліком сучасних фазових детекторів є зміщення частоти налаштування, пов'язане із затримкою поширення сигналів у схемі (завмирання сигналу), що призводить до появи додаткової шумової складової в сигналі помилки фазового детектора та викликає флуктуацію фази на виході контуру ФАПЧ у сталому режимі. Висока шумова складова вихідного сигналу фазового детектора послаблюється фільтром нижніх частот, але це призводить до зниження швидкодії системи ФАПЧ при зміні частоти. Ефективним шляхом усунення зміщення частоти налаштування системи ФАПЧ є обчислення фазової помилки за модулем 2π , на основі модифікованого цифрового фазового детектора з пристроєм оцінки неузгодженості сигналів.

Обчислення фазової помилки за модулем 2π реалізовано шляхом формування на виході цифрового фазового детектора цифрового коду помилки, який приймає значення з множини цілих чисел $0 \dots N$. Межі зміни коду від 0 (000 ... 0) до N (111 ... 1) у цьому випадку відповідатимуть зміни фазової помилки від -2π до 2π , код нульовий помилки $N/2$ (011 ... 1), а код помилки заноситься в пристрій оцінки сигналу неузгодженості.

Таким, чином запропонована система ФАПЧ ефективно вирішує задачі фазової синхронізації в широкому діапазоні частот. Обчислення фазової помилки за модулем 2π в режимі синхронізації виключає зміщення частоти налаштування фазового детектора при завмиранні сигналу та зменшує час входження в синхронізм системи ФАПЧ.

Розроблену систему ФАПЧ з модифікованим цифровим фазовим детектором доцільно використовувати в синтезаторах частоти цифрових модемів у системах радіочастотної ідентифікації для додатків доповненої реальності.

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПЕРСПЕКТИВНИХ ЕЛЕКТРОННИХ ПІДПИСІВ НА ОСНОВІ АЛГЕБРАЇЧНИХ РЕШІТОК ДЛЯ ПОСТКВАНТОВОГО ПЕРІОДУ

На сьогоднішній день вирішується серйозна задача у створенні постквантових криптографічних механізмів електронного підпису (ЕП). Також продовжується конкурс NIST PQC США і зараз проходить 3-й раунд цього конкурсу [1, 5].

На 2-му етапі залишили 9 кандидатів ЕП, а саме: CRYSTALS-DILITHIUM, FALCON, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow та SPHINCS+. Три з них (Dilithium, FALCON, qTeSLA) засновані на стійкості алгебраїчних решіток (Lattice-based), чотири (GeMSS, LUOV, MQDSS, Rainbow) – на основі багатовимірних перетворень (MQ-перетворення), один (SPHINCS+) – на стійкості геш-функції, один (Picnic) – на стійкості геш-функції та блокових потокових шифрів [5].

Як і у минулих змаганнях AES та SHA-3, безпека є найважливішим фактором при оцінці постквантових алгоритмів. NIST має намір стандартизувати постквантові алгоритми відкритого ключа для використання в найрізноманітніших протоколах, таких як безпека транспортного шару (TLS), захищена оболонка (SSH), обмін ключами в Інтернеті (IKE), безпека протоколу Інтернету (IPsec) та Розширення системної безпеки доменного імені (DNSSEC). Схеми оцінюються за безпекою, яку вони забезпечують у програмах.

Під час приймання заявок для конкурсу, заявників заохочували, але не вимагали надання доказів безпеки у відповідних моделях безпеки. Вимоги до стійкості ЕП мають бути сформульовані у відповідності до моделі загроз EUF-CMA (Existentially unforgeable under chosen message attacks), тобто забезпечення захисту від екзистенційної підробки при атаках на основі (адаптивно) вибраного шифртексту [1, 5].

Заявникам було запропоновано надати попередню класифікацію відповідно до визначень, наданих у FRN-Dec16, з акцентом на задоволенні вимог до категорій безпеки, продуктивності та/або алгоритм та реалізації.

Організаторами конкурсу NIST PQC було вирішено порівняти алгоритми-кандидати на перспективні постквантові алгоритми ЕП за трьома критеріями: безпека/стійкість, технічні вимоги до експлуатації та захищеність від атак. За схожими критеріями проводили вибір кандидатів для другого раунду цього конкурсу.

Метою доповіді є дослідження та порівняння двох алгоритмів електронного підпису, які базуються на алгебраїчних решітках, що вийшли у фінал конкурсу NIST PQC.

Дослідження механізму ЕП FALCON

Falcon – це схема підпису на основі решітки. Назва Falcon походить від перших літер того, на чому базується алгоритм, а саме: Fast Fourier lattice-based compact signatures over NTRU (Компактні підписи на основі швидкої вибірки Фур'є поверх NTRU) [2, 4].

Коротко, схема підпису Falcon може бути описана таким чином: Falcon = GPV рамка + решітки NTRU + Швидка вибірка Фур'є.

Безпечність/Стійкість: Істинна вибірка Гауса використовується всередині, що гарантує незначний витік інформації про секретний ключі до практично нескінченного числа підписів (понад 264). Falcon пропонує дуже хороші показники продуктивності. Основна новизна – це дуже швидкий рекурсивний алгоритм вибірки Гауса, при використанні деревоподібної структури даних.

Техніко-експлуатаційні вимоги: Ця структура вимагає двох складових: Клас криптографічних решіток. Обрано клас решіток NTRU.

Захищеність від атак: Найвідоміші атаки на Falcon ґрунтуються на зведенні решітки, без істотного використання спеціальної структури решітки NTRU. Потрібно проводити більше досліджень та вдосконалень, щоб алгоритм підпису був захищений від атак бічними каналами [2, 4].

Дослідження механізму ЕП CRYSTALS-DILITHIUM

Crystals-Dilithium є механізмом електронного підпису на основі решітки, що побудована з використанням методу „Fiat-Shamir з перериваннями” Lyubashevsky, який використовує вибірку відхилення, для того, щоб зробити схеми Fiat-Shamir на основі решіток компактними та безпечними [3].

Основною новизною Crystals-Dilithium є те, що розмір відкритого ключа зменшений майже у 2,5 рази, а для компенсації кожен підпис включає додаткову підказку, що дозволяє перевірити підпис.

Найбільш відомі атаки засновані на зведенні базису решітки без значного використання алгебраїчної задачі.

На нинішній час, Crystals-Dilithium має підтвердження стійкості в моделі випадкового оракула. Цей доказ є нетривіальним і він доводить надійність моделі випадкового оракула.

Підпис Crystals-Dilithium при деяких умовах може забезпечити захист від спеціальних атак, що засновані на використанні витоку інформації по технічних каналах в процесі використання підпису в незахищеному комп'ютері [3].

ВИСНОВКИ

1. Організаторами конкурсу NIST PQC було вирішено порівняти алгоритми-кандидати на перспективні постквантові алгоритми ЕП за трьома критеріями: безпека/стійкість, технічні вимоги до експлуатації та захищеність від атак. За схожими критеріями проводили вибір кандидатів для другого раунду цього конкурсу.

2. Алгоритми, що було розглянуто – Falcon та Crystals-Dilithium, вийшли у другий раунд конкурсу NIST PQC, на рівні з іншими алгоритмами електронного підпису Picnic, qTESLA, Rainbow, SPHINCS, MQDSS, LUOV та GeMSS, обійшовши велику кількість інших кандидатів. А також були обрані до 3-го раунду у якості алгоритмів-фіналістів.

3. Алгоритм Falcon побудовано на комплексі структур: «Компактні підписи на основі швидкої вибірки Фур'є поверх NTRU» (Fast Fourier lattice-based compact signatures over NTRU): Fast Fourier (Швидке перетворення Фур'є), Lattice-based (Криптографія на основі решітки), Compact signatures (Компактний підпис), NTRU-система на основі решітки.

4. Crystals-Dilithium є механізмом електронного підпису на основі решітки, що побудована з використанням методу "Fiat-Shamir з перериваннями" Lyubashevsky, який використовує вибірку відхилення, для того, щоб зробити схеми Fiat-Shamir на основі решіток компактними та безпечними.

ЛІТЕРАТУРА

1. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms, 2016. [Електронний ресурс]. – Режим доступу: <https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms>.
2. FALCON, 2020. [Електронний ресурс]. – Режим доступу: <https://falcon-sign.info/>.
3. Crystals-Dilithium. [Електронний ресурс]. – Режим доступу: <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-3-Submissions>.
4. Prest T. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU / T. Prest, J. Hoffstein, T. Pornin та ін. //, 2020. – Режим доступу: <https://falcon-sign.info/falcon.pdf>.
5. Gorjan Alagic Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8309 / Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone // 22 July 2020. – Режим доступу: <https://doi.org/10.6028/NIST.IR.8309>.

КОНЦЕПЦІЯ ПОБУДОВИ СИСТЕМИ СУПУТНИКОВОГО ЗВ'ЯЗКУ „ЧИСТИЙ КОСМОС”

За допомогою супутникових систем можна здійснювати дослідження земної поверхні та верхніх шарів атмосфери, прогноз землетрусів, екологічний моніторинг, а також будувати системи супутникового зв'язку (ССЗ). Однак створення супутникових систем різного призначення стикається з проблемою космічного сміття, яка з кожним роком стає все більш актуальною.

На навколоземній орбіті за інформацією від різних джерел знаходяться понад 750 тисяч об'єктів, які являють собою не що інше як космічне сміття. У переважній більшості це різні гайки, болти і частки фюзеляжу. Серед них є і величезні старі супутники з ядерними елементами та розгінні блоки, які, як правило, відправляються на спеціальну орбіту поховання.

Існує кілька офіційних орбіт поховання. „Класична” розташовується на 200 км вище геостаціонарної орбіти, де знаходяться тисячі навколоземних супутників. На цю орбіту відправляються відпрацьовані орбітальні апарати для зменшення ймовірності їх зіткнення з робочими об'єктами.

Ще одна найбільша сміттева орбіта для великих супутників знаходиться на висоті від 600 до 1 000 км. На цю орбіту відправляються військові розвідувальні супутники з ядерною енергетичною установкою. Вважається, що частини супутників зможуть перебувати на низькій сміттевій орбіті понад 2 тисячі років, після чого гравітація Землі поступово притягне активні реактори. Однак знаходження навіть на цій орбіті вимагає періодичної корекції траєкторії супутників, без якої їх перебування там може становити серйозну небезпеку і труднощі в подальшому дослідженні космосу.

Зараз тільки 10 % всіх об'єктів космічного сміття фіксуються наземними станціями, а траєкторія їх руху відома. На навколоземних орбітах постійно відбувається так званий ефект Кesslera, коли одні шматочки сміття постійно стикаються з іншими, що призводить до абсолютно неконтрольованого поділу цих об'єктів. Згідно з математичними розрахунками, зіткнення двох космічних частин сміття призводить в середньому до появи ще шести-семи невеликих об'єктів. Вчені вважають, що в майбутньому, якщо людство продовжить з такою швидкістю виводити об'єкти в космос, в тому числі на геостаціонарну орбіту, рано чи пізно станеться каскадний ефект: один космічний об'єкт зіткнеться з іншим, після чого він досить сильно змінює орбіту і стикається з іншими штучними об'єктами, які знаходяться на своїх орбітах. Гіпотетично це може буквально за кілька днів знищити або вивести з ладу всі супутники, створені людьми [1].

Крім того, деякі великі космічні об'єкти, у яких повністю закінчується термін експлуатації, навмисно підривають для того, щоб в подальшому їх невеликі уламки притягувалися Землею і згорали в атмосфері. Однак існують десятки прикладів, коли шматки сміття залишалися на орбітах, як в разі зіткнення двох штучних супутників „Космос-2251” і Iridium 339 в лютому 2009 року або тестування Індією своїх протисупутникових гармат в березні 2019 року.

На сьогоднішній день поки не існує дієвих технологій для боротьби з космічним сміттям, крім відправки супутників на орбіти поховань.

Безліч вчених працюють над створенням систем для утилізації космічного сміття. В основному такі проекти пропонують два рішення проблеми. Перше дозволяє збільшити термін керованого перебування супутників або їх частин, які відпрацьовували свій ресурс, на сміттевій орбіті, але очевидно, що цей термін колись закінчиться. Друге – передбачає створення роботів-збирачів сміття, які будуть його виводити з орбіти Землі. Розвиток таких способів боротьби з космічним сміттям стримується необхідністю значних інвестицій на їх реалізацію, а також відсутністю законодавчої бази в даній сфері на міжнародному рівні.

Для забезпечення ефективного використання штучних апаратів висока вартість їх створення і виведення в космос, як правило, компенсується досить тривалим періодом експлуатації. Крім технічних вимог до розташування супутників на певній висоті, це одна з причин використання середніх і високих орбіт – чим вище орбіта, тим довше на ній може знаходитися супутник. Низькі навколоземні орбіти не можуть забезпечити тривале перебування супутників в космосі без коригування траєкторії руху внаслідок їх досить швидкого зниження, яке викликане гальмуванням апаратів частинками атмосфери, які присутні на таких орбітах. Однак саме низька орбіта здатна забезпечити самоочищення космосу, коли супутники після виконання своєї місії будуть опускатися в атмосферу природним чином і згоряти в ній. Такий підхід вимагає перегляду самих принципів побудови космічних апаратів (КА), оскільки на сьогодні, в своїй переважній більшості, це великогабаритні об'єкти, які не зможуть повністю згоріти при вході в атмосферу.

В даному випадку для створення ССЗ актуальним стає використання КА у вигляді розподіленого супутника, який складається з угруповання над малих КА, відомих під назвою наносупутник (НС) [2].

Важливим етапом створення, підтримання та оновлення ССЗ є процес виведення супутників на орбіту, який, як правило, відбувається за допомогою ракет-носіїв, в тому числі багаторазового використання. Наприклад, останній запуск для поповнення угруповання системі *Iridium* відбувся 11.01.2019 року з космодрому База Ванденберг. За допомогою ракети-носія *Falcon 9* було виведено десять супутників *Iridium NEXT*, вагою 860 кг кожен. Всього протягом 2017-2019 років відбулось вісім запусків *Falcon 9*, що дозволило здійснити виведення 75 апаратів. Зазначений спосіб виведення є досить вартісним, тому лише держави з потужною економікою мають власні ракети-носії.

Альтернативний спосіб виведення супутників на орбіту – повітряний старт, який передбачає запуск космічних апаратів з повітряних суден горизонтального зльоту. Таки переваги, як зменшення маси, сили протидії та вартості ракети-носія, дозволяють у кілька разів знизити витрати на запуск. На сьогодні саме українські літаки АН-124-100 „Руслан” та АН-225 „Мрія” можуть бути задіяні для виконання цієї місії [3].

За рахунок використання розподіленого супутника та повітряного старту ефективність супутникового сегменту на базі НС виявляється значно вищою у порівнянні із існуючими ССЗ. Окрім того, запропоноване рішення в цілому підвищує надійність усієї системи, оскільки втрата або вихід з ладу окремих НС незначним чином вплине на характеристики угруповання, а у випадку часткового резервування НС в кластері такі події можуть бути повністю нівельовані. Немаловажним є і той факт, що з'являється можливість поетапного оновлення космічного сегменту. Використання НС вирішить проблему космічного сміття, оскільки НС будуть знаходитись на низькій орбіті та по закінченні своєї місії будуть повністю згорати в земній атмосфері.

ЛІТЕРАТУРА

1. Святослав Иванов. Орбита захоронения: почему над Землей летают тысячи никому не нужных спутников. /Электронный ресурс/ <https://hightech.fm/2019/08/26/orbita-satellite>.
2. Alexander Lysenko, Valerii Yavisiya, Andrii Tureichuk, Irina Alekseeva. Monitoring system and fixed communication on the basis of nanosatellites //2018 5th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). October 10-13, 2018, Kyiv, Ukraine, pp. 495 – 498.
3. Явіся В.С., Лисенко О.І., Алексеева І.В., Тачиніна О.М. Підхід до побудови космічного сегменту системи супутникового зв'язку CLEAR SPACE // Тринадцята міжнародна науково-технічна конференція „Перспективи телекомунікацій”. Матеріали конференції. – К.: КПІ ім. Ігоря Сікорського. – 2019. – С. 22 – 26. ISSN (print) 2663 – 502X.

СИСТЕМА ФІКСОВАНОГО ЗВ'ЯЗКУ НА БАЗІ КЛАСТЕРІВ НАНОСУПУТНИКІВ

Однією з основних ознак, за якими класифікують сучасні системи супутникового зв'язку (ССЗ), є висота орбіти, на якій розміщуються космічні апарати.

Геостационарні ССЗ мають вищу стабільність рівня сигналу в радіолінії, то при зменшенні висоти орбіти цей показник погіршується через збільшення впливу ефекту Доплера. Однак значна відстань до геостационарної орбіти викликає велике загасання та затримку сигналу. Крім того, геостационарна орбіта вже є перенасиченою та не спроможна забезпечити покриття приполярних областей, тому в перспективі перевага надається низько та середньоробітальним ССЗ.

Прикладом низькоорбітальної ССЗ є система *Iridium*, до складу якої входить 75 супутників на шести орбітах, 20 базових станцій та 2 станції управління і контролю. В поточному році компанією *Iridium Communications Inc* завершено оновлення орбітальної складової системи *Iridium*. Покриття земної поверхні здійснюється шляхом формування окремим супутником *Iridium NEXT* до 48 променів, причому кожен промінь забезпечує обслуговування території з діаметром 700 км. В поточний момент часу для запобігання взаємного впливу сигналів суміжних променів кожним *Iridium NEXT*, в середньому, використовується лише 32 промені [1].

Роботу системи *Iridium* забезпечує 66 апаратів, які знаходяться в активному режимі. Один апарат здійснює покриття території з діаметром 4000 км. При виході з ладу або ушкодженні зазначена зона не може бути повністю обслугована суміжними апаратами. За наявності резервного супутника потрібен певний час на перегрупування апаратів на орбіті, тому впродовж цього терміну не буде забезпечена нормативна якість обслуговування. Звичайне резервування, яке передбачає збільшення кількості супутників може вирішити зазначену проблему, але такий спосіб є досить коштовним. Тому виникає ідея використання в певному сенсі розподіленого апарату, вихід з ладу елементів якого не значним чином вплине на його функціональність в цілому. Така ідея може бути реалізована при використанні над малих космічних апаратів – наносупутників (НС).

Передбачається, що завдання, які виконуються одним апаратом *Iridium NEXT*, можна реалізувати шляхом створення угруповання (кластеру), що має певну кількість НС. Склад кластеру пояснює рис. 1. Для його створення буде необхідно 32 НС, кожен з яких буде формувати один промінь для обслуговування зони з діаметром 700 км. Для взаємодії з іншими кластерами на власній та суміжних орбітах достатньо 4 НС, для передавання сигналів в напрямку наземних станцій – 2 НС, ще 1 НС необхідний для забезпечення взаємодії та управління зазначеними НС, його доцільно дублювати. Тоді загальна кількість НС кластеру дорівнює 40 [2].

При такому підході до побудови космічного сегменту ССЗ масове виробництво НС зменшує собівартість окремого підключення (каналу) у порівнянні з *Iridium NEXT* майже у п'ять разів.

В цілому вартість створення національної ССЗ може бути зменшена за рахунок удосконалення системи виведення на орбіту: використання власних багаторазових ракет-носіїв або запровадження „повітряного старту”. Перший шлях вимагає значних інвестицій і на сьогодні не може бути фінансований державою. В той же час, для розвитку ідеї повітряного старту, який дозволяє у разі зменшити витрати на запуск, в Україні є як відповідні конструкторські розробки, так і фундамент такої системи запуску космічних апаратів – літак Ан-225 „Мрія”. На підтвердження такої ідеї можна навести успішно проведені компанією Virgin Orbit випробування повітряного старту на базі літака Boeing 747 – 400 [3].

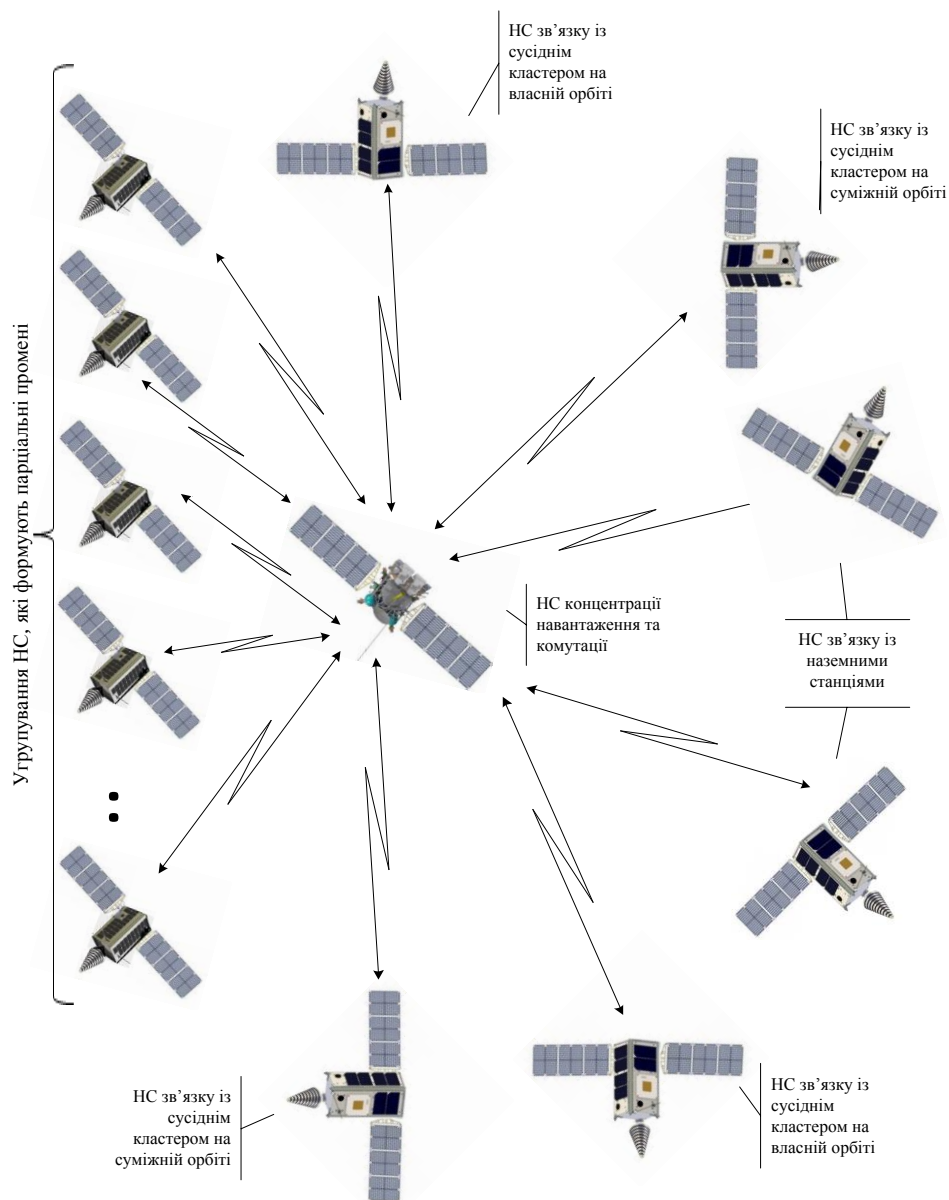


Рис.1. Наносупутниковий кластер

Таким чином, для створення національної ССЗ є доцільним використання функціонально розподілених супутників у вигляді кластерів НС, які виводяться на орбіту за допомогою повітряного старту літаками Ан-225. Також при цьому спрощується процедура оновлення космічного сегменту та вирішується проблема космічного сміття.

ЛІТЕРАТУРА

1. Satlink. Технические характеристики спутниковой системы связи Iridium /Електронний ресурс/ http://www.satlink.ru/Spytnikovaia_sviaz/Iridium/Tehnicheskie_harakteristiki.html.
2. Alexander Lysenko, Valerii Yavisya, Andrii Tureichuk, Irina Alekseeva. Monitoring system and fixed communication on the basis of nanosatellites //2018 5th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). October 10-13, 2018, Kharkiv, Ukraine, pp. 495 – 498.
3. Повітряний старт. Virgin Orbit успішно запустила ракету-носіє з літака. /Електронний ресурс/ <https://uazmi.org/news/post/ghvjbxmN6zT3F7w4QYohsU>.

Литвинюк Б.В. (в/ч А2022)
Воробйов А.О. (в/ч А2022)
Шпачинський Є.О. (в/ч А1942)
Морозов А.Є. (в/ч А2022)
к.т.н. Хижняк І.А. (ХНУПС)

ПРОПОЗИЦІЇ ЩОДО ПЕРЕОБЛАДНАННЯ МАШИНИ СТАРШОГО ОФІЦЕРА БАТАРЕЇ УПРАВЛІННЯ АРТИЛЕРІЙСЬКИМ ВОГНЕМ НОВІТНІМИ ЗАСОБАМИ ЗВ'ЯЗКУ СИЛАМИ РЕМОНТНОГО ПІДРОЗДІЛУ ЧАСТИНИ

На сьогоднішній день в Збройних Силах України йде глибока модернізація та переобладнання військової техніки новітніми засобами зв'язку, але спроможностей оборонного-промислового комплексу недостатньо для переобладнання всієї техніки в короткі строки. Виходячи з цього пропонується варіант переобладнання машини старшого офіцера батареї силами ремонтного підрозділу частини та екіпажем, який надалі забезпечить спроможності щодо виконання завдань за призначенням до моменту модернізації вказаної машини управління на підприємствах оборонно-промислового комплексу України.

Використання новітніх засобів зв'язку на відміну від засобів зв'язку старого парку значно підвищують ефективність функціонування системи управління підрозділами, їх мобільність та захист від засобів радіоелектронної розвідки противника.

Досвід застосування підрозділів артилерії під час виконання завдань в операції Об'єднаних сил вказує на те, що артилерійська батарея може виконувати завдання як в складі дивізіону, так і самостійно в ролі артилерійського резерву. В разі виконання завдання в якості артилерійського резерву існує велика необхідність в каналі радіозв'язку на відстані, що не забезпечують засоби УКХ радіозв'язку. Тому для цього надаються засоби КХ радіозв'язку, а саме радіостанції виробництва компанії HARRIS (MPR9600). Також під час застосування вищевказаних підрозділів суттєвим фактором є їх висока мобільність, що визначає безпосередньо їх живучість.

Враховуючи вищевказане та відсутність новітніх зразків машин управління артилерійським вогнем існує потреба уніфікації використання наявних засобів зв'язку артилерійської батареї в польових умовах, а саме встановлення засобів зв'язку безпосередньо в машині управління, що забезпечить їх постійну готовність до роботи та зменшить час на їх підготовку.

Наведено перелік виробів, які зазвичай входять до складу засобів зв'язку. Визначені завдання, що покладаються на наявні засоби зв'язку.

Враховуючи вищевказане встановлення засобів зв'язку доцільно проводити безпосередньо на робочому місці оператора зв'язку, що забезпечить оперативне керування ними. Для кріплення засобів зв'язку з металу виготовляються спеціальні конструкції з прижимним механізмом, що забезпечить їх швидкий демонтаж в разі потреби використання не в складі машини управління, а в заглибленому об'єкті.

Для забезпечення можливості маневру антенами виходячи з ситуації що склалася, антенні входи виносяться на борт машини в місці де виключений вплив зовнішнього середовища (окислення, запікання тощо) в нашому випадку для цього підходить штатне місце ТК-2 з легким польовим кабелем. Це місце забезпечує використання найкоротших коаксіальних з'єднань до борту машини та відокремлення траси їх прокладання від трас прокладання силових ліній.

Лінії виведення антенних входів доцільно прокладати коаксіальним кабелем. Краще для цього використовувати кабель, що забезпечує найбільш менше затухання та має опір 50 Ом. З можливих кабелів потрібно розглядати кабелі RG-58, RG-213. Блок антенних виходів обладнано з перехідників UHF female – UHF female які вмонтовуються безпосередньо в корпус машини. Траса прокладання коаксіальних кабелів повинна бути відокремлені від ліній електроживлення обладнання, вразі неможливості при паралельному

проходженні паралельне відокремлення не менше 20 см, а вразі перетину тільки під прямим кутом (перпендикулярно).

При встановленні радіостанцій MOTOROLA DM4600 треба враховувати можливість використання зовнішніх антен (направлена антена, колінеарна антена) та автомобільних антен, що закріплюються на криші автомобіля. Направлена антена при підйомі її на щоглу для зв'язку з кореспондентом на значному віддаленні під'єднується до блоку антенних входів за допомогою штатного кабелю RG-213. Радіостанції встановлюються під стелю автомобіля на штатні кріплення.

При встановленні радіостанції HARRIS MPR-9600 враховується можливість зняття її з посадкового місця для періодичної заміни АКБ та застосування окремо. В комплекті відсутній фідер та пристрій з'єднання фідера з плечима штатного диполу. При розгортанні антени диполь від борту автомобіля доцільно використовувати кабель RG-213, який має менший рівень згасання. Практично було перевірено, що прокладена траса по кунгу 5 м та 10 м фідеру від роз'єму UHF від борту машини до пристрою живлення диполу забезпечують належний рівень VSWR в діапазоні від 1,0:1-1,5:1 (залежить від ширини діапазону частотного плану), в разі збільшення показника VSWR потрібно виконати зменшення або збільшення плеч диполу (1 плече повинно відповідати $\frac{1}{4}$ довжини робочої хвилі). Пристрій живлення плеч диполу виконується на діелектричній основі (як варіант пластикова водопровідна труба). Фідер безпосередньо вмонтовується в трубу з попередньо виготовленими відводами в різні боки екраном та центральною жилою не більше 5 см на бокові кріплення плеч диполу. Після під'єднання заливаються діелектричним матеріалом. Такий варіант розгортання антени забезпечує конфігурацію антени як в вигляді перевернутої V так і диполу для роботи випромінюванням в зеніт на відстані до 500 км. Також можливо конфігурувати антену для роботи відбитою хвилею від іоносфери з орієнтуванням на кореспондента на відстані від 500 км.

Встановлення ретранслятора "Либідь К-2РТД" повинно забезпечувати обзорність вбудованих сигналізаторів (індикаторів) та можливість оперативної комутації антенно-фідерного обладнання (вибір дуплексера та варіанту роботи ретранслятора на дві антени чи на одну через дуплексер). На антенний блок від борту автомобіля комутуються виходи грозозахистів вбудованих в ретранслятор. Для можливості використання ретранслятора в якості однорангово в мережі IP site connect старшого начальника під'єднуються заздалегідь прокладеною витою парою, що веде до комунікаційного обладнання.

Антенний вихід тактичного комплексу супутникового зв'язку виводиться до блоку антенних входів. В безпосередній близькості від комплексу супутникового зв'язку встановлюється комутаційна коробка на 8 входів RG-45, що з'єднується з зовнішньою комутаційною коробкою. Комутаційна коробка встановлюється з метою забезпечення швидкої комутації цифрового каналу від модему супутникового зв'язку. Комутація конфігурується в залежності від завдання.

З метою забезпечення живлення засобів зв'язку доцільно врахувати можливість підключення до промислової однофазної мережі напругою 220 В. Резервне живлення машини забезпечується від малогабаритного однофазного дизельного генератора вихідною напругою 220 В. При обладнанні вхідного роз'єму потрібно врахувати можливість надання транзитного живлення для чого обладнується паралельний транзитний вихід. Кабель живлення прокладається до банку розеток, що встановлюється на робочому місці оператора. Для забезпечення безперебійної роботи радіостанції DM4600 до блоку ДЖС -12-15 паралельно під'єднується АКБ призначений для обладнання машини управління.

Для забезпечення в подальшому встановлення виробу криптографічного захисту відводиться відокремлене місце в металевому ящику та з виконаною комутацією до маршрутизатора тактичного комплексу супутникового зв'язку.

Таким чином надані пропозиції щодо переобладнання новітніми засобами зв'язку силами ремонтного підрозділу частини машини старшого офіцера батареї управління артилерійським вогнем, які фактично відповідають визначеним завданням.

ОСНОВНІ ЗАКОНОДАВЧІ ДОКУМЕНТИ З РЕГУЛЮВАННЯ ПИТАНЬ КІБЕРБЕЗПЕКИ В УКРАЇНІ ТА СВІТІ

Поняття „кібербезпека” у широкому загалі застосовується відносно недавно. Однак широта і зміст цього поняття набули великого резонансу у світі, де повсякчас відбувається розвиток інформаційних технологій, інформатизації, комп’ютеризації та глобального інформаційного простору, що, своєю чергою, призвело до збільшення кількості кіберзагроз.

Основним рішучим кроком на шляху подолання кіберзагроз в Україні став прийнятий Закон „Про основні засади забезпечення кібербезпеки України” від 9 травня 2018 року № 2163-VIII. Новий закон спрямований на формування загальної державної політики кібербезпеки, а також розподіл функцій між різними відомствами. Зокрема, він дає повноваження спецслужбам для кіберзахисту країни [1].

Ще однією подією для України є розпочата розробка фахівцями Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України (далі – РНБО) Стратегії кібербезпеки України. Ця Стратегія дасть змогу посилити кіберзахист країни, а також визначити пріоритети національних інтересів України у сфері кібербезпеки і основні підходи та напрями до формування питань кіберзахисту. Указом Президента України № 392 введене в дію рішення РНБО України від 14 вересня 2020 року „Про Стратегію національної безпеки України” [2].

Стратегії більшості країн серед основних загроз національним кіберпросторам визначають:

- кібершпигунство та військові дії, які ведуться за підтримки або з відома держави. Усі технологічно розвинені держави та корпорації стають об’єктом кібершпигунства, яке має на меті заволодіти державними або промисловими таємницями, персональними даними або іншою цінною інформацією;

- використання Інтернету в терористичних цілях;

- кіберзлочинність: викрадення персональних даних та відмивання коштів, отриманих незаконним шляхом.

Відповідно, національні законодавства країн, як правило, регулюють питання захисту:

- персональних даних (Канада, Нідерланди, Естонія, Швеція, Фінляндія, Іспанія);

- електронної комерції та безпеки електронних транзакцій і платіжних інструментів (США, Канада, Польща, Естонія, Італія);

- важливих об’єктів інфраструктури та інформаційних систем (Франція).

Стратегія кібербезпеки Європейського Союзу (далі – ЄС) 2013 року стала першим всеохоплюючим документом ЄС у цій сфері. Документ охоплює всі аспекти кіберпростору: внутрішній ринок, правосуддя, внутрішню та зовнішню політику. Разом зі Стратегією була розроблена та прийнята законодавча пропозиція про посилення безпеки інформаційних систем ЄС. Пріоритетами міжнародної політики ЄС у кіберпросторі, як їх визначає Стратегія, є:

- свобода та відкритість (стратегія визначає принципи користування основоположними правами людини та громадянина в кіберпросторі);

- застосування законодавства ЄС у кіберпросторі тією самою мірою, як і у фізичному світі. Відповідальність за безпеку кіберпростору лежить на усьому суспільстві – від пересічних громадян до держави в цілому;

- розвиток потенціалу кібербезпеки через співробітництво з міжнародними партнерами та організаціями, приватним сектором та громадянами [3].

Слід зазначити, що питання українського і міжнародного законодавства з кіберзахисту є надзвичайно актуальним. Досвід іноземних держав у сфері кіберзахисту є на порядок вищим. Це свідчить про необхідність розроблення та впровадження в Україні регулюючих нормативних документів із захисту від кіберберзагроз у кіберпросторі.

З метою розроблення максимально ефективних інструментів боротьби з кіберзагрозами важливою є взаємодія України з іншими державами. Необхідність створення цих інструментів зумовлена такими факторами:

- активне зростання кіберзлочинів, кібератак та інших дій злочинців;
- наявна так звана «кібервійна» між провідними країнами світу в кіберпросторі;
- відсутність механізму державних політик із кібербезпеки, який би враховував швидкоплинність та розвиток глобальних тенденцій сьогодення;
- відсутність міжнародної правової бази, яка б сприяла розвитку співробітництва між державами.

Головним завданням європейських та й інших країн світу є проведення заходів, що дасть змогу зменшити (а подекуди – унеможливити) негативні наслідки від кібератак. Значну роль у виробленні єдиних підходів щодо забезпечення кібернетичної безпеки як складової національної безпеки європейських країн відіграє ЄС.

Рекомендації ЄС щодо кібербезпеки в законодавчому та загальному форматі такі: впорядкування чинної законодавчої бази; забезпечення стабільності мережі Інтернет шляхом вироблення керівних принципів; захист критичної інформації в інфраструктурі; навчання (підвищення рівня знань та обмін досвідом); дослідження актуальних проблем у сфері кіберзахисту; співпраця між державами (міжнародні форуми, конференції, наради, ділові зустрічі); посилення контролю за інформаційним простором для завчасного реагування на кіберзагрозу та спільного подолання її.

У перспективі Україна повинна стати активним учасником цих безпекових процесів. Це сприятиме закріпленню іміджу держави та формуванню більш посиленого законодавчого та організаційного фундаменту національної кібербезпеки.

ЛІТЕРАТУРА

1. Піскорська Г.А. Сучасні виклики і загрози в кіберпросторі: формування механізму міжнародної інформаційної безпеки [Електронний ресурс] / Г.А. Піскорська, Н.Л. Яковенко. – Режим доступу: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3389.
2. У РНБО розробляють Стратегію кібербезпеки України [Електронний ресурс]. – Режим доступу: <https://armyinform.com.ua/2020/09/u-rnbo-rozroblyayut-strategiyu-kiberbezpeky-ukrayiny>.
3. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших [Електронний ресурс]. Режим доступу: <https://parlament.org.ua/wp-content/uploads/2016/11/INFODOVIDKA-ZAKONODAVSTVO-TA-STRATEGIYI-KIBERBEZPEKA.pdf>.

РЕОРГАНІЗАЦІЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ В УМОВАХ КІБЕРВЛИВУ ІЗ ЗАСТОСУВАННЯМ НЕЙРОНОМЕРЕЖЕВОЇ ТЕХНОЛОГІЇ

Існування людини в сучасному світі не можливо уявити без використання інформаційно-телекомунікаційних систем. Адже саме інформаційно-телекомунікаційні системи (ІТС) забезпечують своєчасне збирання, пошук, оброблення та пересилання інформації з метою забезпечення інформаційних потреб користувачів.

ІТС являють собою розподілені, багато ієрархічні (гетерогенні) системи мереж, програм та пристроїв, які взаємодіють між собою з метою обміну інформацією, її зберігання та обробки. Працездатність ІТС залежить від стійкості функціонування її телекомунікаційної складової, а саме телекомунікаційних мереж. Збільшення навантаження на мережі, їх постійне організаційне ускладнення та поява новітніх методів порушення роботи, у т.ч. в кіберпросторі, створюють необхідність дієвого відношення до проблем трансформації телекомунікаційних систем, мережевого захисту, а саме кіберзахисту.

Стійкість функціонування ІТС в умовах кібервпливу не можливо представити без такої функції трансформації, як реорганізаційна, а саме: здатності забезпечити функціонування ІТС при виході з ладу її ресурсів за рахунок перерозподілу функцій складових, які втрачені, між працездатними, які функціонують далі. Реорганізаційна функція тісно пов'язана з процесом самоорганізації телекомунікаційних мереж (ТМ). Саме вплив (зовнішній чи внутрішній) на ТМ переводить її із стану спокою в стан нерівноваги, який являється необхідною умовою для розвитку. Тільки тоді нелінійні динамічні мережі об'єднуються, нове утворення не рівне сумі частин (так як деякі з них зазнали впливу та були втрачені), а створює мережу другої організації або систему іншого рівня.

Для опису телекомунікаційних мереж, що переходять від невпорядкованого до стану спокою (рівноваги в процесі функціонування) використовується узагальнений математичний апарат синергетики.

В стані, далекому від рівноваги, починають діяти біфуркаційні механізми (зміна числа чи типу стаціонарних точок ТМ). Фундаментальним принципом самоорганізації є поява нового порядку та ускладнення систем через флуктуації (випадкові відхилення) стану їх елементів та підсистем, що можуть бути обумовлені впливом дестабілізуючого фактору (у т.ч. і кібервпливу). Оскільки флуктуації носять випадковий характер, то стан системи після біфуркації обумовлено дією суми випадкових факторів.

Найбільш ефективним підходом до оцінювання функцій трансформаційних можливостей ТМ є побудова математичної моделі ІТС із застосування системи штучного інтелекту, а саме нейрономережевої технології. Саме нейронні мережі набули широкого поширення завдяки здатності адаптуватися до різного роду ситуаційних завдань, контролю (оцінювання) та управління. Перевагою зазначеної моделі є можливість одержання нової інформації про проблемну область з у формі деякого прогнозу, недоліком – представлення знань про проблемну область у спеціальному виді, яке може суттєво відрізнятися від можливої змістовної інтерпретації існуючих зв'язків і відносин. Створення нечітких нейронних мереж (гібридних) об'єднує в собі переваги нейронних мереж і систем нечіткого висновку (обчислювальні технології).

Таким чином використання ТМ саме без сталої структури та здатних трансформуватися, адаптуватися до змінних характеристик транспортної мережі, використовуючи гібридні алгоритми маршрутизації (проактивна та реактивна), гібридної нейрономережевої технології дозволить підвищити стійкість функціонування ІТС в умовах кібервпливу.

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ ГЕОПРОСТОРОВОГО ОБЛІКУ ТА КОНТРОЛЮ ЗЕМЕЛЬ ТА ІНШОГО НЕРУХОМОГО ВІЙСЬКОВОГО (ДЕРЖАВНОГО) МАЙНА МОУ

Актуальність дослідження обумовлена необхідністю вдосконалення системи геопросторового обліку та контролю земель та іншого нерухомого військового (державного) майна МОУ.

Системи геопросторового обліку та контролю земель та іншого нерухомого військового (державного) майна МОУ має складну та неоднорідну структуру з різними програмним забезпеченням в більшості випадків ПЗ є застарілим, що робить цю систему досить заплутаною та повільною. Питання масштабування для системи є болючим із за її складної структури та безлічі залежностей в підсистемах.

Мета дослідження полягає у підвищенні ефективності механізмів обліку та контролю земель та іншого нерухомого військового (державного) майна МОУ, за рахунок виконання наступних часткових завдань дослідження:

- аналіз особливостей обліку та контролю земель та іншого нерухомого військового (державного) майна МОУ;
- аналіз сучасних наукових підходів у застосуванні СППР на основі використання методів *ML* для виконання задач підвищення ефективності механізмів обліку та контролю земель та іншого нерухомого військового (державного) майна МОУ;
- вдосконалення існуючої моделі СППР, з урахуванням її недоліків та обмежень;
- автоматизація процесів обліку та контролю земель та іншого нерухомого військового (державного) майна МОУ за рахунок розробки програмного модулю підтримки прийняття рішення з використанням методів машинного навчання в системі геопросторового обліку та контролю земель та іншого нерухомого військового (державного) майна МОУ “Ground and Building Control”.

Виклад основного матеріалу. Було з’ясовано, в якому неприйнятному стані в Збройних силах перебуває процесу обліку нерухомого майна. Незважаючи на локальні спроби автоматизувати цей процес, він залишається досить заплутаним та повільним. Оцінивши досвід інших країн, можна прийти до висновку, що Збройним силам необхідна відповідна централізована система, що має гарно стати до нагоди усьому процесу „диджиталізації” країни. Визначено загальне завдання системи, і, як наслідок, часткові задачі створення системи для даної роботи.

Одне з основних завдань системи геопросторового обліку та контролю земель та іншого нерухомого військового (державного) майна МОУ є аналіз та передбачення виконаних робіт. Рішення даного завдання являє собою складний процес, який включає в себе збір даних, їх аналіз, узгодження формату для даних, виокремлення оптимальної вибірки, тренування моделі передбачення та підбір глобальних параметрів.

Базуючись на етапи проектування структури системи, використовуючи класичний підхід проектування було розроблено узагальнену архітектуру і алгоритми роботи та базову модель програмного модулю підтримки прийняття рішення з використанням методів машинного навчання в системі геопросторового обліку та контролю земель та іншого нерухомого військового (державного) майна МОУ.

Висновки. Отже, в роботі запропоновано використання метод машинного навчання бінарної класифікації *Two-Class Boosted Decision Tree* для проектування моделі передбачення на його основі реалізовано програмний модуль підтримки прийняття рішення з використанням методів машинного навчання в системі геопросторового обліку та контролю земель та іншого нерухомого військового (державного) майна МОУ. Даний модуль інтегрований з СПЗ “Ground and Building Control”.

АНАЛІЗ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗАПОБІГАННЮ ВИТОКУ ІНФОРМАЦІЇ З ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

На сьогоднішній день повсюдне використання автоматизованих систем для зберігання, обробки і передачі інформації призводить до загострення проблем, пов'язаних з їх захистом. Вважається, що однією з найбільш небезпечних загроз є витік конфіденційної інформації що зберігається і оброблюється всередині автоматизованої системи і джерелом небезпеки є внутрішні співробітники. Але частіше найбільшу увагу приділяють зовнішнім загрозам: спаму і фішингу, атакам типу „відмова в обслуговуванні”, вірусам, підміні головних сторінок Інтернет-ресурсів, шпигунському та рекламному програмному забезпеченню, соціальній інженерії. Натомість практика показує, що внутрішні загрози здатні заподіяти куди більш серйозної шкоди, ніж зовнішні. Все це змушує більш пильно розглянути можливі способи захисту від витоку інформації з середини.

Для протидії витоку інформації через використання внутрішніх загроз застосовується система DLP (Data Loss Prevention) – система запобігання витоку даних. Принцип роботи DLP-системи полягає в аналізі всієї інформації: вихідної, вхідної і тієї, що циркулює всередині компанії. Система аналізує, що це за інформація і в разі, якщо вона є критичною і відправляється туди куди не належить – система блокує передачу і/або повідомляє про це співробітника служби захисту інформації. За здатністю блокування передачі інформації, впізнаної як критична, виділяють системи з активним і пасивним контролем дій користувача. Активні блокують передачу інформації при виявленні порушень, а пасивні системи, тільки фіксують підозрілі факти, оформляючи їх у звіти для подальшого аналізу з боку служби захисту інформації.

Основні функції DLP системи:

- контроль передачі інформації через Інтернет з використанням E-Mail, HTTP, HTTPS, FTP, Skype, ICQ та інших додатків і протоколів;
- контроль збереження інформації на зовнішні носії, CD, DVD, flash, мобільні телефони;
- захист інформації від витоку шляхом контролю виведення даних на друк;
- блокування спроб пересилання/збереження конфіденційних даних, інформування служби захисту інформації про інциденти, створення тінювих копій;
- пошук конфіденційної інформації на робочих станціях і файлових серверах за ключовими словами, мітками документів, атрибутами файлів і цифровими відбитками;

Додавання DLP до системи кібербезпеки надає наступні переваги:

- запобігання внутрішніх і зовнішніх загроз витоку інформації;
- забезпечення видимості обміну даними;
- застосування процедур авторизації перед доступом до критичних даних;
- застосування машинного навчання для виявлення ненормальної поведінки користувача та маркування критичних даних.

Недоліки використання DLP системи:

- розгортання DLP вимагає багато часу і зусиль;
- необхідні точні політики до протоколів передачі даних;
- створення політики запобігання втраті даних займає багато часу;
- можуть виникнути складнощі з підготовкою інвентаризації всіх критичних даних і установкою прав користувача.

Вивчення варіантів застосування та вибір їх раціонального варіанту є метою подальших досліджень.

ВАРІАНТ ЗАСТОСУВАННЯ СИСТЕМ ЗАПОБІГАННЯ ВТОРГНЕНЬ В ІТС У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

В останні декілька років відбувся і триває надалі розвиток в організації та застосуванні систем та методів захисту інформації в інформаційно-телекомунікаційних системах (ІТС) Збройних Сил України. Одним із найважливіших факторів реалізації раціонального захисту вважається виявлення „уразливостей” в інформаційній системі. Для цього у Збройних Силах України впроваджується використання програмних засобів – систем запобігання вторгнень (Intrusion Prevention System, IPS).

Використовують як безкоштовні програмні засоби, такі як OpenVAS, Netmap, так і платні – такі як Nessus, Nexpose в поєднанні з Metasploit. Ці програмні засоби здатні виявити уразливості в системі, провести попередній аналіз їх можливого впливу на систему, створити звіт по рівнях деталізації та надати інформацію про можливі шляхи усунення знайдених уразливостей.

Існує два основних механізми, за допомогою яких сканери перевіряють наявність уразливості – активний та пасивний моніторинг.

Пасивний моніторинг – механізм пасивного аналізу, за допомогою якого сканер намагається визначити наявність уразливості із „прослуханого” в мережі трафіку, без фактичного підтвердження її наявності, тобто за непрямыми ознаками. Процес пасивного моніторингу ідентифікує трафік за портами (службами, на транспортному рівні), знайдені на кожному мережному пристрої, і збирає пов’язані з портами заголовки, отримані в процесі „прослуховування” мережі. Кожен отриманий заголовок порівнюється з таблицею правил визначення мережних пристроїв, операційних систем і потенційних уразливостей. На основі проведеного порівняння робиться висновок про наявність чи відсутність уразливості.

Активний моніторинг – механізм активного впливу та аналізу відповіді елементів системи. Активний моніторинг виконується шляхом імітації атаки або її частини, і на основі реакції системи робиться висновок про наявність чи відсутність уразливості. Такий активний вплив на елементи системи може іноді призвести до порушення працездатності її елементів. Проведення активного моніторингу впливає на працездатність мережі, але цей метод пошуку вразливостей більш точний у результатах їх пошуку.

Для інформування адміністраторів інформаційно-телекомунікаційних систем створюються різноманітні бази даних уразливостей програмного та апаратного забезпечення. Наприклад:

- Національна база даних уразливостей (National Vulnerability Database) США;
- Common Vulnerabilities and Exposures (Загальна база вразливостей та ризиків), яку підтримує організація MITRE.

З досвіду роботи можливо сказати – найпоширенішими уразливостями у ЗС України є:

- використання слабких паролів або паролів по замовчуванню;
- неоновлене антивірусне програмне забезпечення та операційні системи;
- наявність запущених без необхідності використання мережних служб;
- нехтування використанням міжмережних екранів;
- скачування файлів та встановлення ПЗ із неавторизованих джерел;
- використання програм-взломників захисту ліцензійних прав, які майже повністю є носіями зловмисного програмного коду, т. д.

Ці уразливості ставлять загрозу кібезбезпеці ЗС України і потребують постійного контролю. З цією метою в центрах кіберзахисту ЗС України використовують сканери безпеки, але їх застосування має періодичний характер. Для вдосконалення процесу пошуку вразливостей слід використовувати системи активного моніторингу на системній основі. Дослідження цього питання є напрямком подальших досліджень.

РОЗПІЗНАВАННЯ КОМП'ЮТЕРНИХ ВІРУСІВ ЗА ДОПОМОГОЮ НЕЙРОННИХ МЕРЕЖ

Актуальність дослідження обумовлена необхідністю вдосконалення системи захисту інформації та кібернетичної безпеки Збройних Сил України в цілому, а саме спосіб уникнення використання стороннього антивірусного програмного забезпечення, придбання ліцензій на його використання та залежності від швидкості оновлення антивірусних баз, що, як наслідок, підвищує рівень захищеності інформації.

Антивірусне програмне забезпечення потребує значної витрати часу при пошуку загроз на носіях інформації та оновленні самих баз антивірусного програмного забезпечення, які не є актуальними на момент появи нового комп'ютерного вірусу, що служить загрозою для безпеки інформації. Нейронні мережі значно спрощують цей процес можливістю складання припущень на основі масиву даних, використаного для навчання, які, у свою чергу, дозволяють випереджувати швидкість появи нових вірусів та мати захист до самої їх появи.

Мета дослідження полягає у підвищенні ефективності процесів розпізнавання комп'ютерних вірусів та захисту інформації за рахунок виконання **наступних часткових завдань дослідження**:

- аналіз сучасного підходу у захисті інформації та наявних засобів розпізнавання комп'ютерних вірусів у Збройних Силах України, спираючись на вимоги керівних документів;
- пошук готових моделей нейронних мереж та порівняння їх між собою, розгляд можливості та раціональності створення власної з урахуванням потреб в сфері захисту інформації, аналіз мов програмування, бібліотек та сучасних засобів щодо забезпечення навчання та створення нейронної мережі;
- безпосереднє створення моделі нейронної мережі, її навчання та підбір оптимального масиву даних, апробація та створення програмного забезпечення для автоматизації розпізнавання комп'ютерних вірусів за допомогою нейронної мережі;
- тестування програмного забезпечення на основі підготовлених заражених файлів для визначення його ефективності у сфері захисту інформації;

Виклад основного матеріалу. Одною з основних проблем захисту інформації є наявність та постійне удосконалення вірусного програмного забезпечення. Компанії та організації, які займаються його розробкою, на даний момент, мають можливість лише постійно відслідковувати появу нових вірусів та додавати їх у базу, з якою у подальшому мають синхронізуватися користувачі антивірусного програмного забезпечення, що, як правило, може стати летальним у захисті інформації і означати її втрату. Нейронна мережа займається прогнозуванням, що при дійсному навчанні дає можливість запобігати і розпізнавати віруси на етапі їх появи та у деякому сенсі ще до неї.

Основною метою даної роботи є дослідження сучасних засобів для захисту інформації у сфері розпізнавання комп'ютерних вірусів та розроблення програмного забезпечення на базі високоточної моделі нейронної мережі для забезпечення швидкості пошуку та розпізнаванні їх на ранніх етапах роботи.

Висновки. Отже, в роботі проаналізовано наявні засоби захисту інформації від комп'ютерних вірусів, досліджено засоби їх створення на прикладі мов програмування, готових моделей та бібліотек для автоматизації процесів створення та навчання нейронних мереж. На основі цього запропоновано використання нейронної мережі у якості основи для розпізнавання комп'ютерних вірусів та реалізація програмного забезпечення для зручності та автоматизації задач, пов'язаних з пошуком, проведенням сканування файлів та винесення свого рішення на основі виданих нейронною мережею відповідей.

ОПТИМІЗАЦІЯ РОБОТИ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ НА ПУНКТАХ УПРАВЛІННЯ ПІД ЧАС ВИКОНАННЯ ОПЕРАЦІЙ (БОЙОВИХ ДІЙ)

З початком проведення АТО (ООС) великої необхідності та актуальності набуло питання щодо управління військами та інформування підрозділів про зміни в обстановці яка склалася. Для забезпечення управління військами, їх взаємодії, взаємного обміну інформацією між пунктами управління (далі – ПУ) і їх елементами під час підготовки та в ході операції (бойових дій) створюються та розгортається система зв'язку та спостереження.

Метою удосконалення система зв'язку та спостереження є впровадження в практику нових технічних засобів. Одним із таких засобів являється камери відео спостереження (відеокамери). На даний час відеокамери (далі – ВК) широко використовуються під час проведення ООС, як ефективний засіб отримання інформації та спостереження за обстановкою.

До основних переваг такого засобу спостереження належить: можливість одному оператору спостерігати одразу за декількома ділянками місцевості; довгострокова автономність ВК (не потребує постійного обслуговування); виявлення противника з використанням засобів маскування; вести відеозаписи обстановки, які використовуються для розвідувальних даних; при наявності спеціального програмного забезпечення дає змогу розвідувати противника (цілі противника) з визначенням його положення (координат); проводити розвідку в режимі нічного бачення.

ВК являють собою цілу систему відеоспостереження яка працюють автономно та у режимі on-line передаючи відео – інформацію оператору. Для забезпечення передачі відеоряду застосовується АСУ „Дніпро” з використанням, провайдера „Інтертелеком” та ліній радіорелейного зв'язку (P-402, Air Grid, Ubiguti). До складу системи відеоспостереження, крім ВК входить ПЕОМ підключеного до АСУ „Дніпро“, та обладнання для передачі сигналів по радіорелейних лініях зв'язку (P-402, Air Grid, Ubiguti). Підключивши ВК до АСУ „Дніпро” надається можливість дистанційного моніторингу працездатності відеокамер через ПЕОМ, де використовуються додаток zabbix, friendly pinger які проводять перевірку обміну даних з визначеним ір-адресами пристроїв. Дана система відеоспостереження постійно удосконалюється, але існує ряд проблемних питань, таких як: явна недостатня кількість кваліфікованих спеціалістів серед військовослужбовців та ІТ – спеціалістів, які здатні фахово встановити, налаштувати, підключити та продіагностувати ВК; відсутність цільової програми фінансування підрозділів, що здійснюють монтаж та обслуговування ВК; явна недостача сучасних радіорелейних станцій, спроможних забезпечити високу швидкість передачі даних на відстань до 30-60 км; низька швидкість передачі даних, що значною мірою пов'язано з тим, що більшість каналів передачі інформації орендуються в приватних компаніях, де трапляються поломки обладнання і т.ін.; майже повна відсутність сучасних систем автономного живлення, заснованих, наприклад, на сонячних панелях. Пропозиції щодо поліпшення роботи системи відеоспостереження є: забезпечення кожного регіонального підрозділу, відповідального за встановлення ВК, кваліфікованим ІТ – фахівцем із передачі відео даних; більш широко використовувати військовий супутниковий Internet для безперебійного швидкого зв'язку; достатньою мірою забезпечити місця виконання завдань сучасним радіорелейним зв'язком; забезпечити широке використання сучасних систем автономного живлення (заснованих переважно на сонячних батареях). Як висновок можна виділити можливість ефективного використання системи відеоспостереження під час виконання завдань в ООС. Впровадження в практику такої системи як елемент нових технічних засобів управління. Це викликає необхідність переглянути в оптимізація роботи системи відео спостереження та надання нових рекомендацій щодо роботи системи у відповідність з сучасними вимогами.

МЕТОДИ МАРШРУТИЗАЦІЇ ТРАФІКУ В СЕНСОРНИХ МЕРЕЖАХ З ВИКОРИСТАННЯМ ЕЛЕМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ

В умовах швидкого розвитку телекомунікаційних та інформаційних технологій, автоматизації процесів управління все більшої популярності набирають безпроводові технології. Безпроводові сенсорні мережі (БСМ) – новий клас мереж, що складається з мініатюрних обчислювано-комунікаційних пристроїв, розподілених певним чином на досліджуваній території які виконують функції збору, аналізу та передачі даних. Як правило БСМ застосовують для таких задач як:

- у військовій сфері (моніторинг бойових дій в реальному часі);
- у цивільній сфері (для локалізації випадків стихійного лиха).

Завданням методу маршрутизації БСМ є створення, зберігання та підтримання заданої якості маршруту між відправником і адресатом в реальному часі в момент динамічної зміни структури вузлів сенсорної мережі.

Тому для забезпечення заданої якості передачі пакетів даних в БСМ пред'являються наступні вимоги:

- процес динамічної варіації (адаптивного підлаштування) оптимального пошуку маршруту БСМ в реальному часі ускладнюється із обмеженням фізичних параметрів сенсорних вузлів мережі;
- пропускна спроможність та швидкість доставки пакетів між адресатами знижується, під час пошуку резервних вузлів БСМ;
- вихід з ладу окремих вузлів не повинен впливати на роботу мережі.

Крім того необхідно враховувати обмеження по часовому інтервалу роботи кожного вузла сенсорної мережі, що залежить від ємності вбудованої батареї.

Тому з урахуванням вище зазначених вимог пропонується концепція, щодо застосування нейромережевого алгоритму *Self-Organization Recurrent Neural Network* (SORNN), для параметризації БСМ в процесі автоматичного пошуку та вибору методу маршрутизації в залежності від умов (під час виникнення невизначених завдань, тощо) в задачах адаптивного підлаштування сенсорних вузлів для побудови динамічної мережевої структури моделі.

Класифікація методів маршрутизації, представлена на рис. 1.

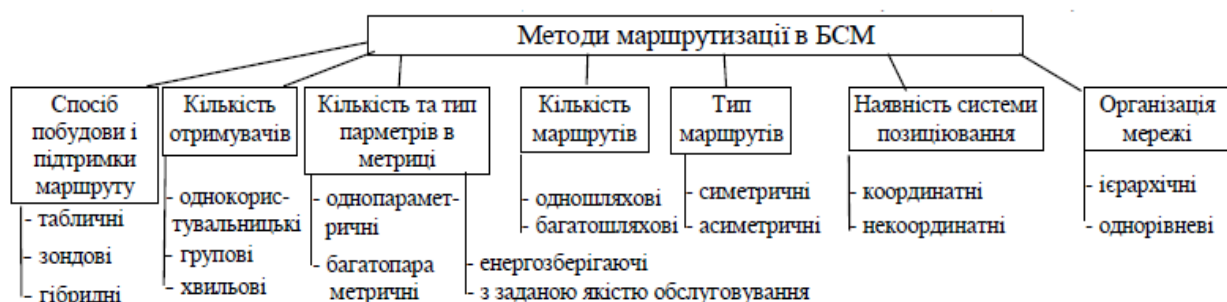


Рис1. Класифікація методів маршрутизації в БСМ

Таким чином застосуванням нейромережевого алгоритму (SORNN) для вирішення вище зазначених завдань дозволить наступне:

- класифікувати сенсорні вузли БСМ за наявністю пошкоджень на фізичному та програмному рівні;
- здійснювати параметризацію вхідних даних сенсорних вузлів в реальному часі ,що дозволить зменшити час на пошук адаптивної структури мережі БСМ;
- зменшення часу на прогнозування застосування резервних вузлів сенсорної мережі.

Мартинюк В.В. (ВІТІ)
Паламарчук Н.А. (ВІТІ)
Паламарчук С.А. (ВІТІ)
Черниш Ю.О. (ВІТІ)

ДЕЯКІ ЗАДАЧІ З ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Функціонування об'єктів критичної інфраструктури (ОКІ) в такому специфічному середовищі, як кіберпростір, пов'язане з уразливістю і загрозами і вимагає розробки нового інструментарію. Поряд з інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб. Неодмінною умовою вирішення питань щодо забезпечення інформаційної та кібербезпеки ОКІ є розуміння того, що держава знаходиться в нерозривному зв'язку і взаємодії з іншими структурами і суб'єктами, що відображається законодавчими, організаційними та технічними (технологічними) аспектами/рівнями взаємодії. В межах зазначених аспектів пропонуються наступні задачі з вдосконалення інформаційної та кібернетичної безпеки ОКІ [1, 2]:

1) розробка та прийняття національних нормативних документів:

Переліку об'єктів критичної інфраструктури держави;

Плану заходів щодо реалізації Стратегії кібербезпеки України;

Протоколу спільних дій основних суб'єктів забезпечення кібербезпеки, суб'єктів кіберзахисту та власників (розпорядників) ОКІ під час попередження, виявлення, припинення кібератак та кіберінцидентів.

2) організаційне узгодження діяльності суб'єктів забезпечення інформаційної та кібернетичної безпеки ОКІ, а саме:

розробка відомчих документів щодо визначення вимог до кіберзахисту ОКІ;

визначення повноважень посадових осіб (введення підрозділів), відповідальних за забезпечення інформаційної та кібернетичної безпеки;

визначення порядку ведення та використання державного реєстру кіберінцидентів.

3) технічне забезпечення інформаційної та кібернетичної безпеки ОКІ:

створення систем забезпечення безпеки ОКІ згідно нормативних (відомчих) документів;

визначення показників забезпечення інформаційної та кібернетичної безпеки ОКІ;

адаптація засобів управління інформацією і подіями безпеки відповідним вимогам;

формалізація підходів керування ОКІ з врахуванням вимог відомчих документів.

Висновки. Комплексна реалізація зазначених задач дозволить забезпечити ефективну інформаційну та кібернетичну безпеку ОКІ шляхом виконання низки правових, організаційних, технічних, наукових заходів, всебічного забезпечення на національному та відомчому рівнях. Подальші дослідження доцільно спрямувати на оцінювання організаційних та технічних аспектів функціонування відомчого ОКІ, з метою повноцінного виконання вимог кіберзахисту та кібербезпеки.

ЛІТЕРАТУРА

1. Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 “Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури”.

2. Мартинюк В.В., Паламарчук Н.А., Паламарчук С.А., Сівоха О.М. Задачі вдосконалення інформаційної та кібернетичної безпеки об'єктів критичної інфраструктури. Збірник наукових праць ВІТІ, № 2, 2020, стор. 54-63.

РОЗВИТОК ШТУЧНИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ ДЛЯ РОЗПІЗНАВАННЯ ОБРАЗІВ

Цифрова обробка сигналів (ЦОС) є одним з найбільш перспективних науково-технічних напрямків в області передачі, прийому та обробки інформації. Область застосування цифрової обробки сигналів постійно розширюється. Впровадження цифрових методів у телекомунікаційних системах здійснюється шляхом переходу до вирішення типових задач цифровими методами, а також шляхом розробки нових методів передачі та обробки інформації.

Швидкий розвиток технологій ЦОС обумовлений не тільки успіхом в розробці нових алгоритмів, але і стрімким прогресом технології виготовлення надвеликих інтегральних схем (НВІС). Сучасні дослідження в теорії ЦОС та НВІС-технології суттєво змінили склад і архітектуру комп'ютерних систем ЦОС. В теперішній час для реалізації алгоритмів ЦОС застосовуються комп'ютерні системи з нетрадиційною архітектурою, що складаються з великої кількості спеціалізованих і функціонально орієнтованих процесорів. Подальший розвиток архітектури комп'ютерних систем ЦОС тісно пов'язаний з розвитком НВІС-технології, яка дозволяє зменшити енергоспоживання, масогабаритні характеристики, підвищити швидкодію та стимулює розвиток одних підходів проектування і забороняє інші.

Розвиток елементної бази та обчислювальної потужності систем дозволяє використовувати їх для побудови складних систем з елементами штучного інтелекту, в тому числі в системах спеціального призначення. Разом з тим, створення штучних систем розпізнавання образів залишається складною теоретичною й технічною проблемою. Основними напрямками розвитку систем штучного інтелекту є нейронні мережі, експертні системи, природномовні системи, еволюційні обчислення, СУБД, що самоорганізуються, інтелектуальна інженерія. Напрямок „нейронні мережі” стабільно тримається на першому місці, що пояснюється потенціалом їх розвитку, перспективою реалізації, а також універсальністю їх роботи в різних сферах.

Традиційно задачі розпізнавання образів включають у коло задач штучного інтелекту, який в свою чергу побудований на нейронній мережі. Важливою властивістю нейронних мереж, що свідчить про їх великий потенціал і широкі прикладні можливості – паралельна обробка інформації одночасно великою кількістю нейронів. Завдяки цьому досягається значне пришвидшення обробки інформації. Іншою, не менш важливою особливістю нейронних мереж, є здатність до навчання та узагальнення інформації. Таким чином досягається деяка схожість з роботою головного мозку людини.

Особлива привабливість нейронних мереж полягає в тому, що їх застосування, завдяки так званому навчанню на наявних даних, дає можливість прогнозувати, які значення прийматимуть досліджуванні змінні у нових спостереженнях, ґрунтуючись на даних попередніх спостережень. При грамотному застосуванні інструментарію нейронних мереж точність таких прогнозів значно перевищує точність прогнозів, здійснених за допомогою інших, зокрема класичних статистичних методів. Завдання прогнозування вирішується нейронними мережами аналогічно завданню розпізнавання образів, а умовою застосування нейромереж в прогнозуванні є наявність “історичних даних”, використовуючи які мережа може „навчатися”.

Авторами пропонується напрямок розвитку штучних систем розпізнавання образів у системах спеціального призначення з використанням нейронних мереж. Використання таких систем дозволить отримувати високу швидкість обробки інформації, а при недостатній кількості даних – найточніше прогнозувати найімовірніший результат.

ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ У ЗАСОБАХ ТРОПОСФЕРНОГО ЗВ'ЯЗКУ

Головною метою розвитку системи зв'язку Збройних сил України є створення єдиного інформаційно-телекомунікаційного середовища на основі впровадження сучасних інформаційно-телекомунікаційних технологій, протоколів обміну інформацією, комплексів, систем та засобів зв'язку спеціального призначення, що дасть можливість забезпечити обмін усім видами інформації між органами й пунктами управління (всіх ланок) з відповідною пропускнуою спроможністю, достовірністю та надійністю.

В ході стратегічного розгортання та застосування Збройних Сил України, а також в ході виконання завдань в операції Об'єднаних сил та антитерористичній операції, виникла критична ситуація щодо забезпечення зв'язком службових осіб на пунктах управління у випадках виходу з ладу стаціонарної компоненти системи зв'язку Збройних Сил України. В таких випадках, для забезпечення зв'язку у оперативній і стратегічній ланках управління стає нагальним використання радіозасобів КХ-діапазону, супутникового зв'язку та засобів тропосферного зв'язку.

Тропосферний зв'язок – радіозв'язок, що здійснюється відбиттям та розсіюванням радіохвиль на неоднорідностях тропосфери між станціями, які знаходяться поза межами прямої видимості.

Принципальна відмінність ліній тропосферного зв'язку від радіорелейних ліній полягає у відсутності прямої видимості. За допомогою тропосферних станцій можна забезпечити зв'язок без ретрансляції на 150–200–250 км, скоротити час на розгортання ліній великої потужності і таким чином зменшити потребу в техніці та особовому складі. Сигнали, які передаються тропосферними станціями, приходять в пункт прийому в значній мірі послаблені. Тому використання тропосферного зв'язку можливо за умови наявності потужних передавачів, високочутливих приймачів, а також антен з великою площею розкриття.

За результатами проведеного аналізу застосування тропосферних засобів у розвинутих країнах світу слід зазначити, що найбільш доцільним є перехід на принципово нові телекомунікаційні технології, які б з одного боку дозволили забезпечити передавання зростаючих обсягів інформації, а з іншого здійснювали б це на екологічно безпечному рівні для особового складу із урахуванням вимог щодо перешкодозахищеності та розвідзахищеності зв'язку. Перехід на нову модель (стратегію) розвитку, що одержала назву моделі стійкого розвитку, є вкрай актуальним і необхідним рішенням та представляється природною реакцією щодо створення тропосферних радіорелейних систем нового покоління з використанням новітніх радіотехнологій на екологічно безпечних і ресурсозберігаючих принципах.

Таким чином, в ході досліджень планується удосконалити сучасні методи цифрової обробки сигналів та розробити пропозиції щодо використання тропосферних станцій нового покоління для створення єдиної інформаційно-телекомунікаційної мережі передачі інформації та підсистем забезпечення автоматизації процесів оперативної діяльності, в тому числі створення автоматизованої системи управління авіацією та протиповітряної оборони Збройних Сил України, автоматизації процесів адміністративно-господарської діяльності, тощо, що у сукупності дозволить створити передумови подальшого розвитку системи військового зв'язку з метою забезпечення роботи перспективної системи управління.

МЕТОДИ ПІДВИЩЕННЯ СТІЙКОСТІ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ДО КВАНТОВИХ АТАК

Актуальність. Стрімкий розвиток та глобальне впровадження новітніх інформаційних технологій, зокрема, систем електронного документообігу змінює як економіку, так й індустрію по всьому світу. Використання інформаційних технологій у всіх сферах життя суспільства робить досить актуальною проблему захисту інформації, інформаційних ресурсів, каналів передачі даних від злочинних дій зловмисників, зокрема реалізації квантових атак. Але, упроваджуючи СЕД не можна забувати про безпеку цієї системи. Слід брати до уваги той факт, що впровадження захисту призводить до ускладнення в роботі системи, зниження її ефективності, тому впровадження системи захисту повинно бути обґрунтованим і доцільним.

Мета. Метою роботи є підвищення стійкості квантостійкого алгоритму SPHINCS⁺, який буде застосовуватися для криптографічного захисту СЕД.

Основна частина. На даний час було проведено значну кількість досліджень у сфері квантових обчислень, які використовують квантові механічні явища для розв'язування математичних задач, важких або нерозв'язних для звичайних комп'ютерів. Якщо найближчим часом будуть побудовані масштабні квантові комп'ютери, вони зможуть зламати багато криптосистем з відкритим ключем, які зараз використовуються на практиці. Це становить значну загрозу конфіденційності та цілісності цифрових комунікацій в Інтернеті. Метою постквантової криптографії є розробка криптографічних систем, захищених як від квантових, так і класичних комп'ютерів, які можуть взаємодіяти з існуючими протоколами зв'язку та мережами.

Національний університет стандартизації та технологій США (NIST) ініціював процес пошуку, оцінки та стандартизації одного або декількох квантостійких криптографічних алгоритмів. За висновками першого етапу виділили 26 кватостійких алгоритмів, які увійшли до другого етапу. При аналізі даних алгоритмів можна виділити криптосистеми на основі геш-функцій. Клас алгоритмів, збудованих на геш-функціях, має найкоротші ключі та високу швидкодію з-поміж усіх інших кандидатів конкурсу. Такі алгоритми є достатньо непоганим вирішенням завдання криптографічного захисту систем електронного документообігу до квантових атак.

Пост-квантовий алгоритм електронного цифрового підпису SPHINCS⁺ заснований на трьох варіантах геш-функцій: SHA-256, SHAKE-256 та Haraka. Однак, для використання даного алгоритму в Україні необхідно використовувати національні криптографічні стандарти, наприклад, ДСТУ 7564:2014 "Інформаційні технології. Криптографічний захист інформації. Функція гешування", який визначає геш-функцію „Купина”. Пропонується створити нову специфікацію алгоритму SPHINCS⁺ на основі геш-функції “Купина”, що очікувано підвищить криптостійкість та надасть можливість впроваджувати пост-квантово стійкі системи криптографічного захисту за національними стандартами України.

Висновок. Було проаналізовано кожен з алгоритмів, які пройшли до другого туру конкурсу, який проводиться в NIST. Найбільш доцільним захистом СЕД є алгоритми з великою швидкодією; саме тому вибір алгоритмів скоротився до алгоритмів на основі геш-функцій. Аналіз алгоритмів, які залишилися показав, що алгоритм SPHINCS⁺ є досить надійним, щоб забезпечити безпеку СЕД на найближче майбутнє.

Методом підвищення криптостійкості алгоритму SPHINCS⁺, який в подальшому буде використовуватися для цифрового підпису електронних документів є створення нової специфікації SPHINCS⁺-Купина з більш надійною основою за допомогою ДСТУ 7564:2014. Це підвищить надійність СЕД з появою нових атак на основі квантових обчислень.

МОДЕЛЬ ВІДМОВИСТОЙКОГО КЛАСТЕРА ВІРТУАЛІЗАЦІЇ З МОЖЛИВІСТЮ „ГАРЯЧОЇ” МІГРАЦІЇ ВІРТУАЛЬНИХ МАШИН

У сучасному світі все більше набирають популярність хмарні технології. Але також слід зауважити, що є конкретні проблеми з переходом на хмарні технології, наприклад, робота сервісів та програмного забезпечення від різних виробників для різних платформ. Разом з тим, застосування хмарних технологій передбачає застосування технології віртуалізації. При цьому слід врахувати такі параметри, як швидкодія віртуального середовища, навантаження на систему, простота розгортання тощо. Для вирішення цих проблем застосовуються різноманітні функції міграції у віртуальному середовищі.

Ефективність системи управління віртуальними машинами полягає у використанні комбінацій різних алгоритмів міграції. Це дозволяє вирішити проблему простоїв та неефективного використання обчислювальних ресурсів. Також система управління міграцією дозволяє досягти низької щільності обчислювальних процесів на одиницю фізичного сервера, знімаючи необхідність в окремому сервері, виділеному для виконання того чи іншого користувацького завдання.

Беручи до уваги вищезазначене, було проведено аналіз програмного забезпечення технології віртуалізації, та на основі даного аналізу було обрано програмне забезпечення віртуалізації з відкритим вихідним кодом *Proxmox VE*, яке надає ключові наступні можливості:

- просте управління через веб-інтерфейс;
- моніторинг навантаження в реальному часі;
- бібліотека інсталяційних образів (в локальному або віддаленому сховищі);
- підключення до «фізичної» консолі гостьових систем безпосередньо з браузера (по VNC);
- об'єднання серверів в кластер з можливістю динамічної міграції віртуальних машин (без зупинки гостьової системи);
- швидке розгортання гостьових систем з шаблонів (доступно тільки для *OpenVZ*);
- автоматичне резервне копіювання віртуальних машин;
- дозволяє забезпечити віддалені запуски в роботу нових філій;
- забезпечення можливістю установки і перестановки операційних систем без необхідності фізичної присутності системного адміністратора;
- забезпечення можливістю швидкої заміни серверного обладнання без переривання роботи філії (“гаряча” міграція).

Висновки

Важливість технологій віртуалізації для сучасної обчислювальної техніки навряд чи можна переоцінити, і цій галузі, як і будь-який інший, розвивається настільки ж динамічно, конкуренція компаній-розробників і їх продуктів йде тільки на користь. А розробка додаткових інструментів і засобів, які дозволяють автоматизувати або просто зробити більш зручною роботу з фундаментальними технологіями

За допомогою цієї системи адміністратори центрів обробки даних зможуть більш якісно обслуговувати навантаження на сервери. А також дозволить переносити віртуальні машини з одного центру обробки даних в інший, без втрати даних, та зупинки систем що розгорнуті на тих машинах. Що забезпечить високодоступність, зменшить час відмови систем що розгорнуті в датацентрі.

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ХМАРНОГО СЕРЕДОВИЩА НА БАЗІ РІШЕННЯ CISCO CLOUDLOCK

Хмарні технології, як набір засобів, що виконує обчислення за допомогою віддалених серверів і програм без безпосереднього залучення ресурсів комп'ютера користувача, грає важливу роль у робочих процесах в корпоративному сегменті.

Актуальність дослідження новітніх методів забезпечення безпеки в хмарному середовищі зумовлено проблемами безпеки та конфіденційності, що виникають у користувачів. Не враховуючи класичні ризики безпеки, що виникають у подібних системах, хмарні системи мають специфічні проблеми безпеки та конфіденційності через віртуалізацію хмар та характер своєї багаторівневої інфраструктури.

На даний момент часу хмарні технології потребують автоматизовані заходи запобігання витоку даних та дотримання нормативних вимог регулювання. Для підвищення рівня інформаційної безпеки в хмарному середовищі необхідно застосувати комплексний підхід, що зможе вирішити проблему конфіденційності та захищеності користувачів, даних та додатків в рамках хмарного середовища.

Реалізація комплексного підходу кібернетичної безпеки у хмарному середовищі можлива на базі рішення Cisco CloudLock – брокеру безпеки доступу до хмарного середовища (CASB).

Ключові функції:

безпека користувачів;

захист даних;

безпека додатків;

автоматизований моніторинг тіньової IT-інфраструктури;

дозвіл на експлуатацію (ATO) за програмою FedRAMP для Cloudlock.

Cisco CloudLock – це унікальне рішення безпеки доступу до хмарного середовища (Cloud Access Security Broker), що забезпечує кібернетичну безпеку в хмарній системі. Функціонал, що включений до брокеру, захищає користувачів, дані і додатки в рамках хмарних систем. Cloudlock використовує APIs для управління ризиками в екосистемі хмарних додатків. У рішенні Cloudlock інтегровані сучасні алгоритми машинного навчання, що розпізнають несанкціоновану діяльність, виходячи з налаштованого набору параметрів. Технологія запобігання витоку даних (Data Leak Prevention), що є складовою у Cloudlock, здійснює безперервний моніторинг хмарних середовищ, створюючи умови для своєчасного виявлення і захисту конфіденційної інформації. Міжмережевий екран додатків Cloudlock розпізнає будь які хмарні додатки, що підключені до корпоративного середовища і має керування цими додатками.

Також є можливість дізнатися створений рейтинг довіри спільноти (Community Trust Rating) та розрізнити їх в залежності від ризику. Однією з переваг є доступність програми Office на будь-якому пристрої та в будь-якому браузері, а також в онлайн режимі та автономно.

Отже, питання кібернетичної безпеки є одним з найактуальнішим на сьогоднішній день, тому рішення, що надає контроль за діями користувачів, безпекою додатків та збереженню даних є нагальною потребою в корпоративному світі. Cisco CloudLock відповідає на питання проблематики захисту інформації в хмарному середовищі.

Завдяки комплексному підходу, брокер забезпечує конфіденційність даних та є одним з найкращих рівень в організаціях різних сфер, що мають на меті збереження конфіденційності інформації.

АНАЛІЗ МОДЕЛЕЙ ОЦІНКИ ТА МЕТОДІВ ПІДВИЩЕННЯ НАДІЙНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМ УПРАВЛІННЯ ВІЙСЬКАМИ ТА ОЗБРОЄННЯМ

Револьюційні 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 військами 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, які застосовуються у системі управління військами та озброєнням.

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, супроводжуваністю 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.

Оцінка надійності ПЗ суттєво відрізняється від існуючих методів розрахунку надійності складних технічних систем тому, що відмови програмного забезпечення мають іншу природу і не залежать від умов експлуатації, зовнішнього оточення, фізичного старіння і зносу елементів і інших причин, характерних для матеріальних об'єктів. При оцінці і аналізі надійності технічної системи моделі надійності її елементів, як правило, відомі, так як вони визначаються на етапі їх розробки та виготовлення. При цьому визначення надійності елементів проводиться шляхом перевірки досить великого числа цих елементів, з фіксацією збоїв і відмов. Такі моделі надійності елементів дозволяють отримати оцінку надійності всього пристрою.

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 не відбувається.

Всі моделі надійності можна класифікувати за тим, який із перерахованих процесів вони підтримують (пророкують, прогнозують, вимірюють тощо). Потрібно відзначити, що моделі надійності, які в якості вихідної інформації використовують дані про інтервали між відмовами, можна віднести і до вимірюючих, і до оцінюючих в рівній мірі. Деякі моделі засновані на інформації, яка отримана в ході тестування ПЗ, дають можливість робити прогнози поведінки ПЗ в процесі експлуатації.

Аналітичні моделі дають можливість розраховувати кількісні показники надійності, ґрунтуючись на даних про поведінку програми в процесі тестування (вимірюють і оцінюють моделі). Емпіричні моделі базуються на аналізі структурних особливостей програм. Вони розглядають залежність показників надійності від числа міжмодульних зв'язків, кількості циклів в модулях тощо. Часто емпіричні моделі не дають кінцевих результатів показників надійності, проте вони включені в класифікаційну схему, так як розвиток цих моделей

дозволяє виявляти взаємозв'язок між складністю систем управління військами та озброєнням і його надійністю. Ці моделі можна використовувати на етапі проектування ПЗ, коли здійснюється розбивка на модулі і відома його структура.

Аналітичні моделі представлені двома групами: динамічні моделі і статичні. У динамічних, поведінка ПЗ (поява відмов) розглядається в часі. У статичних моделях поява відмов не пов'язана з часом, а враховується тільки залежність кількості помилок від числа тестових прогонів (за областю помилок) або залежність кількості помилок від характеристики вхідних даних (за областю даних). Для використання динамічних моделей необхідно мати дані про появу відмов у часі. Якщо фіксуються інтервали кожної відмови, то виходить безперервна картина появи відмов у часі (група динамічних моделей з безперервним часом). З іншого боку, може фіксуватися тільки число відмов за довільний інтервал часу.

Отже, аналіз існуючих моделей надійності програмного забезпечення (моделі Шумана, Ла Падула, Желінського-Моранді, Шика-Волвертона, Муса, Мілса, Ліпова, Коркорена, Нельсона, модель прехідних ймовірностей, проста інтуїтивна модель тощо) показує, що вони є неадекватними до реального процесу 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 (недоцільне).

Між програмними помилками, відмовами та надійністю програмного забезпечення 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, так як проявляються не самі програмні помилки, а їх результат – відмова; програмні помилки можуть впливати одна на одну, тому після виправлення однієї програмної помилки можуть з'являтися 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 і застосування спеціальних, додаткових методів підвищення надійності ПЗ (оперативний захист від ненавмисних, випадкових спотворень обчислювального процесу, програм і даних), які призначені для виявлення і 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 надлишковості 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-х кратного резервування продуктивності окремої машини в багатопроцесорних обчислювальних системах. На практиці до засобів, які використовують тимчасову надмірність можна віднести авторизацію доступу користувачів до системи, аналіз доступних користувачеві ресурсів, виділення ресурсів відповідно до ролям і рівнями підготовки користувачів, розмежування прав доступу користувачів до окремих завдань, функцій управління, записів і полів баз даних.

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. До засобів забезпечення надійності, що використовують інформаційну надмірність можна віднести посилкову цілісність баз даних, яка забезпечується за рахунок системи внутрішніх унікальних ключів для всіх інформаційних записів системи, відкрита система кодування, що дозволяє користувачеві в будь-який момент змінювати коди будь-яких об'єктів класифікації, механізми перевірки значень контрольних сум записів системи, забезпечують виявлення всіх несанкціонованих модифікацій інформації.

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 надмірності 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 і 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.

ПЕРСПЕКТИВИ ТА МОЖЛИВОСТІ ЗАСТОСУВАННЯ ПІДСИСТЕМИ ВИЗНАЧЕННЯ СТІЙКОСТІ СИСТЕМИ ЗБЕРЕЖЕННЯ ДАНИХ

Актуальність обраної теми доповіді полягає в тому, що сьогодні людство існує та функціонує у світі систем, який в свою чергу так само є глобальною системою з мільйонними розгалуженнями та багатоструктурними зв'язками. І всі без винятку галузі людської діяльності існують та функціонують саме у системі. ЗСУ так само не є виключенням, навіть навпаки, Збройні Сили функціонують лише в налагодженій, з чітким алгоритмом дій, системі. І моніторинг та злагодженість роботи цієї системи в автоматизованому режимі це одне із актуальних завдань процесів модернізації ЗСУ. Формальне рішення зазначеного завдання полягає в тому, що вводиться деякий комплексний критерій якості, тобто деякий математичний вираз, який дозволяє зіставити безлічі числових характеристик, що описують систему, деяке число, що визначає якість цієї системи.

Мета дослідження полягає у з'ясуванні перспектив проектування та можливостей практичної реалізації і подальшого використання підсистем визначення стійкості системи збереження даних з метою модернізації процесів функціонування ЗСУ за рахунок виконання наступних завдань:

- дослідження та аналіз можливостей проектування та практичної реалізації підсистем визначення стійкості системи збереження даних у ЗСУ, визначення особливостей функціонування таких підсистем для ЗСУ;

- дослідження та аналіз актуальності даного питання та винесення, на основі отриманих результатів аналітичних робіт, висновків щодо доцільності його втілення в реальність в сучасних умовах розвитку ЗСУ.

Виклад основного матеріалу. Система зберігання даних (СЗД) є комплексом програмних і апаратних засобів, створених для управління і зберігання великих обсягів інформації. Основним сховищем інформації в малих компаніях є файлові сервери і сервери СУБД, дані яких зберігаються на локальних жорстких дисках. У великих компаніях обсяги інформації можуть досягати сотень терабайт. Саме тому великі компанії впроваджують системи зберігання даних (СЗД). Що стосується ЗСУ, то роки паперового діловодства створили своєрідну систему у силових структурах нашої держави. І один із головних недоліків цієї системи, яких є доволі багато, це необхідність оперування фізичними об'єктами, що значно сповільнює більшість пов'язаних між собою процесів (обмін інформацією, прийняття рішень, оновлення даних, тощо). Запровадження електронних систем зберігання даних надає можливість застосування величезної гнучкості в обробці та зберіганні інформації, а також стимулює підвищення ефективності та швидкості виконання тих чи інших завдань, наприклад: можливість приймання рішення командирами та віддавання наказів відповідно до швидкої зміни ситуації в режимі реального часу. Уже сьогодні використання таких систем обміну даними є вкрай необхідним для подальшого існування у цифровому світі. Адже швидкість прийняття правильного рішення є запорукою успіху виконання поставлених бойових завдань та збереження життя військовослужбовців.

Висновки. Отже, було з'ясовано та висвітлено основні потреби модернізації у процесах збереження даних в ЗСУ та можливості їх практичної реалізації за допомогою використання можливостей системи зберігання даних. На основі проведених аналітичних та дослідницьких робіт і з'ясованих фактів було зроблено висновки про необхідність діджиталізації та оптимізації процесів в ЗСУ, пов'язаних з інформацією та збереженням даних. У ході проведення аналізу вирішень даного проблемного питання було розглянуто декілька можливих варіантів забезпечення актуальних потреб та наведено їх недоліки та переваги.

ПІДСИСТЕМА АНАЛІТИЧНОЇ ОБРОБКИ ДАНИХ ВІДЕОПОТОКУ НА ОСНОВІ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Актуальність дослідження обумовлена необхідністю підвищення ефективності процесу обробки даних відеопотоку в системах відеоспостереження на військових об'єктах.

Питання безпеки військових об'єктів ніколи не втрачало своєї гострої актуальності. Для підвищення рівня захисту того чи іншого військового об'єкта є доцільним використання систем відеоспостереження в поєднанні з сучасними технологіями аналізу відеопотоку.

Такі системи використовуються для забезпечення безпеки на найбільш важливих об'єктах. Їх головне завдання безперервне стеження за територією об'єкта. Використання таких систем майже повністю виключає людський фактор. Спостереження і розпізнавання об'єктів ведуться безперервно та в режимі реального часу.

Мета дослідження полягає в підвищенні ефективності процесу обробки даних відеопотоку в системах відеоспостереження військових об'єктів за рахунок використання сучасних методів машинного навчання.

До часткових завдань дослідження віднесено:

- аналіз існуючих методів пошуку об'єктів різних класів у відеопотоці з використанням методів машинного навчання;
- визначення вимог до підсистеми виявлення та класифікації об'єктів;
- розробка архітектури підсистеми виявлення та класифікації об'єктів у відеопотоці;
- здійснення оцінки результатів розпізнавання у відеопотоці на основі запропонованого рішення.

Виклад основного матеріалу. Автоматизація процесу аналітичної обробки даних відеопотоку є важливою задачею для забезпечення безпеки військових об'єктів, яка дозволяє здійснювати обробку даних за короткі проміжки часу та з високою точністю. Змістом процесу обробки даних відеопотоку є виявлення об'єктів, їх класифікація та підрахунок кількості об'єктів, віднесених до певного класу, за певний проміжок часу.

Одне з основних завдань при створенні підсистеми обробки даних відеопотоку є проектування її структури, яка визначає внутрішню організацію і взаємозв'язки елементів системи. Рішення даної задачі дозволить здійснювати ефективну обробку вхідного відеопотоку, виявлення об'єктів, віднесення їх до одного з класів та їх підрахунок.

В даній роботі для вирішення завдання синтезу підсистеми аналітичної обробки даних відеопотоку на основі методів машинного навчання проведені дослідження використання сучасних бібліотек комп'ютерного зору.

ImageAI є сучасною бібліотекою на мові програмування *Python*, яка дозволяє легко інтегрувати новітні технології машинного навчання в існуючі або нові проекти, використовуючи незначний об'єм коду. Під час оцінки ефективності бібліотека *ImageAI* показала кращі результати при розпізнаванні об'єктів різних класів та в швидкості розпізнавання в порівнянні з іншими сучасними бібліотеками.

При проектуванні структури підсистеми аналітичної обробки даних відеопотоку було запропоновано включити до її складу модуль розпізнавання та аналізу даних на основі зазначеної бібліотеки *ImageAI*.

Висновки. На основі проведених досліджень існуючих методів машинного навчання показана висока ефективність бібліотеки *ImageAI* та запропоновано її використання у складі підсистеми аналітичної обробки даних відеопотоку на об'єктах військового призначення.

ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС РОЗПІЗНАВАННЯ ВІЙСЬКОВОЇ ТЕХНІКИ ПРИ ОБРОБЦІ ВІДЕОПОТОКУ НА БАЗІ *NVIDIA JETSON NANO*

Актуальність. Сучасні технології машинного навчання набувають широкого розповсюдження в різноманітних галузях та застосовуються в програмно-апаратних платформах для розробки дронів різного цільового призначення. Звичайно використання даної технології дуже актуальна для розвитку оборонного сектору ЗСУ.

Мета: розробити програмно-апаратний комплекс для розпізнавання військової техніки за допомогою комп'ютерного зору при використанні штучного інтелекту.

Основні положення. Машинне навчання (*machine learning*) – це підгалузь штучного інтелекту, що досліджує побудову алгоритмів, які можуть навчатися й робити передбачення з даних шляхом побудови моделі з вибірових входів. Для реалізації програмно-апаратного комплексу розпізнавання об'єктів на відео потоці, було проаналізовано декілька архітектур нейронних мереж, а саме згорткові та рекурентні нейронні мережі. На відміну від рекурентної нейронної мережі *Recurrent neural network (RNN)*, яка використовується для аналізу та розпізнавання тексту та мови, згорткова нейронна мережа *Convolutional neural network, (CNN)* найбільше підходить для обробки зображень та відео. Згорткові нейронні мережі – це клас глибинних штучних нейронних мереж, який успішно застосовується до аналізу візуальних зображень.

Ефективність згорткових нейронних мереж при розпізнаванні зображень є однією з основних причин, згідно якої вони користуються великою популярністю. Але, *CNN* повільніша за інші нейронні мережі, так як необхідно використовувати достатньо велику кількість зображень для її тренування (навчання). У якості даних для навчання використовується тренувальна вибірка – це набір прикладів, які ми показуємо системі, щоб вона на їх базі визначила певну закономірність, яка відповідальна за розподіл даних в тренувальній вибірці. Завдяки знаходженню такої закономірності система зможе її використати для ефективного прогнозування відповідей на тестувальній вибірці, при збільшенні кількості вхідних даних для навчання, зростає якість та точність розпізнавання.

В якості програмно-апаратної платформи було обрано мікрокомп'ютер *NVIDIA Jetson Nano*. Це компактний і потужний комп'ютер, який дозволяє паралельно запускати декілька нейронних мереж в додатках для класифікації зображень, розпізнавання об'єктів, сегментації та обробки відео. Операційна система мікрокомп'ютера – *Ubuntu* разом з *NVIDIA JetPack SDK* містить усі сучасні бібліотеки для машинного навчання. Вбудовані бібліотеки являються наборами підпрограм і функцій, написаних на мові *Python*.

Для навчання нейронної мережі, щодо розпізнавання об'єктів військової техніки, було застосовано бібліотеки *Theano*, *TensorFlow* та *Cuda*. *Theano* – це одна із поширених бібліотек низькорівневих операцій для реалізації алгоритмів машинного навчання. Вона реалізує комплексні матричні мультиплікації, швидкі методи згортки з множенням, методи регресії і всю *backend*-логіку роботи нейронних мереж. *Tensorflow* – відкрита програмна бібліотека для машинного навчання, розроблена компанією *Google* для вирішення завдань побудови і тренування нейронної мережі з метою автоматичного знаходження та класифікації образів, досягаючи якості людського сприйняття. *Cuda* – це програмно-апаратна архітектура паралельних обчислень, яка дозволяє істотно збільшити обчислювальну продуктивність завдяки використанню графічних процесорів *NVIDIA*.

Висновок. В роботі було створено програмно-апаратний комплекс розпізнавання військової техніки при обробці відеопотоку на базі мікрокомп'ютера *NVIDIA Jetson Nano*. Для цього було використано згорткові нейронні мережі та бібліотеки машинного навчання *Tensorflow* та *Theano*, що дозволяє покращити швидкість розпізнавання об'єктів на мобільних платформах.

ПІДСИСТЕМА ВЗАЄМОДІЇ З КОРИСТУВАЧЕМ СИСТЕМИ ОБЛІКУ МАТЕРІАЛЬНИХ ЗАСОБІВ ЛАБОРАТОРІЇ ТЗН ВВНЗ

Актуальність. Питання автоматизації обліку матеріальних засобів лабораторії технічного забезпечення навчального процесу ВВНЗ (ТЗН ВВНЗ) є актуальним у зв'язку з обробкою великої кількості різнотипних найменувань, різних років закупки, їх переміщенням між підрозділами (матеріально-відповідальних осіб), періодичною звіркою наявності матеріальних засобів та узагальнення відповідних звітних документів.

З метою покращення ефективності рівня оперативної обробки інформації та генерації звітів та для зменшення часу на рутинні операції посадових осіб лабораторії ТЗН ВВНЗ необхідно розробити архітектуру інформаційної системи на базі сучасних веб-технологій.

Мета дослідження полягає у вдосконаленні процесу обліку матеріальних засобів лабораторії ТЗН ВВНЗ за рахунок виконання наступних часткових завдань дослідження: аналіз існуючих систем для обліку матеріальних засобів (порівняння їх переваг та недоліків); аналіз існуючих сучасних технологій для розробки інформаційних систем обліку матеріальних засобів; аналіз існуючих веб-технологій для розробки клієнтської частини системи обліку матеріальних засобів.

Виклад основного матеріалу. На теперішній час, існують різноманітні інформаційні системи з функціями обліку матеріальних засобів. Однак запропоновані підходи, в основному, стосуються цивільних організацій, що виробляють, експлуатують, реалізують та обліковують матеріальні засоби згідно відповідної нормативно-правової бази. Аналіз їх функціональних можливостей для організації обліку з урахуванням специфіки військових керівних документів не проводився.

Було проведено аналіз таких інформаційних систем обліку як: „Галактика”, „Парус”. Система обліку „Галактика” – система управління підприємством, яка закриває всі основні операційні та управлінські завдання і надає менеджерам різного рівня точну і своєчасну інформацію для прийняття управлінських рішень. Недоліком даної системи обліку є відсутність можливості надбудову функціоналу, крім виправлень інтерфейсу. Система обліку „Парус” призначена для автоматизації бізнес-задач підприємств малого та середнього бізнесу, великих корпорацій та холдингів, а також бюджетних установ і організацій. Недоліком даної системи є висока вартість програмного продукту та потребує навчання персоналу, що теж здійснюється за додаткову плату.

Враховуючі зазначені недоліки, було прийнято рішення про розробку власної інформаційної системи для обліку матеріальних засобів лабораторії ТЗН ВВНЗ.

Було розроблено архітектуру системи обліку матеріальних засобів лабораторії ТЗН ВВНЗ (рис. 1.). Використання запропонованої архітектури має такі переваги: при такій реалізації кожен компонент системи може продовжувати своє функціонування, що забезпечує відмовостійкість системи; простий інтерфейс для кінцевого користувача, для зручного користування без потреби спеціального навчання; за допомогою використання докерів система є легкою в горизонтальному масштабуванні.

Згідно запропонованої архітектури „*Docker Frontend*” – докер в якому розташована підсистема взаємодії з користувачем на основі *JavaScript*-бібліотеки для створення користувацьких інтерфейсів *React* та *JavaScript*-бібліотека для управління станом додатку *Redux*. Друга складова „*Docker Backend*” – докер в якому розташована підсистема обліку та обробки даних на основі *Python*-фреймворку для розробки веб-систем *Django*. Також до складу системи входить база даних „*MSSQL DB*”, де зберігається вся облікова інформація.

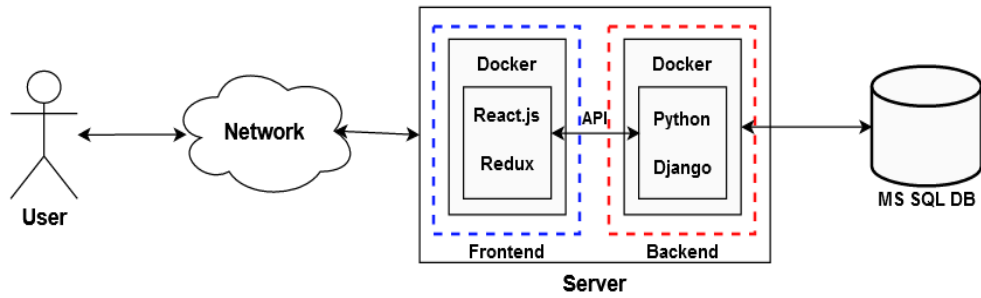


Рис.1 Архітектура системи обліку матеріальних засобів лабораторії ТЗН ВВНЗ

Після синтезу архітектури даної системи було проаналізовано сучасні веб-технології для розробки підсистеми взаємодії з користувачем системи обліку матеріальних засобів лабораторії ТЗН ВВНЗ. Серед сучасних веб-технологій розробки клієнтської частини існує багато фреймворків та бібліотек, які як правило, працюють швидше, витримують більше навантаження, а також мають більший рівень безпеки ніж *Content Management System (CMS)* або самописні системи.

Поміж існуючих фреймворків та бібліотек *JavaScript* набули найбільшу популярність *React*, *Angular* та *Vue*. *Angular* має відносно повільну продуктивність, враховуючи різні показники. *Vue* має недоліки при інтеграції. *React* є швидкою *JavaScript*-бібліотекою, завдяки реалізації *React Virtual Dom* і різним процедурам оптимізації відображення. Також, були проаналізовані бібліотеки для управління стану додатку *Redux* та *MobX*. *Redux* більш легка в налаштуванні та в доступі до стану додатку для різних компонентів в порівнянні з *MobX*. Як результат, проаналізувавши переваги та недоліки сучасних веб-технологій було вирішено використовувати *JavaScript*-бібліотеки *React* та *Redux*.

Після проведення аналізу та вибору технологій для розробки підсистеми взаємодії з користувачем системи обліку матеріальних засобів лабораторії ТЗН ВВНЗ була використана схема візуалізації підсистеми взаємодії з користувачем системи обліку матеріальних засобів ТЗН ВВНЗ (рис. 2.)

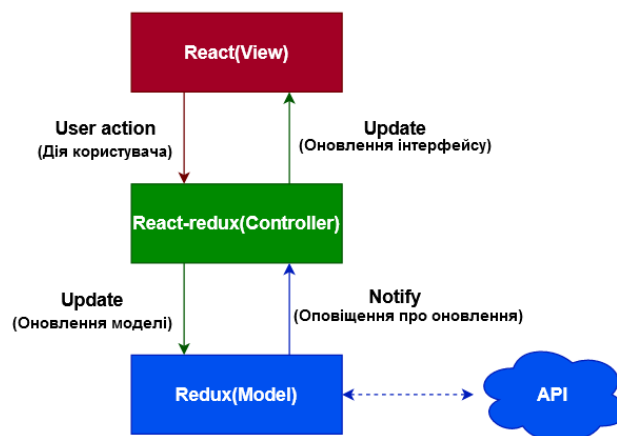


Рис. 2. Візуалізація шаблону проектування MVC за допомогою бібліотек *React* та *Redux*

Висновки. Отже, в рамках даної роботи запропоновано використання шаблону проектування *MVC*, на основі бібліотек *React* та *Redux* для розробки підсистеми взаємодії з користувачем системи обліку матеріальних засобів лабораторії ТЗН ВВНЗ. Також була розроблена архітектура даної інформаційної системи. Реалізація обраних веб-технологій забезпечить наявність зручного інтерфейсу користувача, модульність, що дозволить в подальшому надбудовувати додатковий функціонал та мінімізує затрати часу для обробки інформації та генерації звітів.

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ УПРАВЛІННЯ ЕЛЕМЕНТАМИ ВІРТУАЛЬНОЇ МЕРЕЖІ НА БАЗІ ПРОТОКОЛУ *OPENFLOW*

Актуальність теми: Сучасний етап розвитку комп'ютерних систем можна охарактеризувати зростанням ролі розподілених мережевих клієнт-серверних архітектур унаслідок зниження темпів зростання продуктивності окремих вузлів та необхідністю організації їх спільної роботи для досягнення заданих показників мережевих характеристик. Однією із перспективних технологій є *SDN (Software Defined Networks)*, яка дозволяє централізовано конфігурувати та управляти вузлами мережі, підвищити швидкість відновлення мережі у випадку аварійних ситуацій та відокремити процес передачі даних від вирішення задач управління через стандартизовані інтерфейси на базі протоколу *OpenFlow*.

Мета: Створення віртуальної мережевої моделі *SDN* мережі та розробка програмно-апаратного модуля призначеного для організації управління на базі протоколу *OpenFlow*.

Виходячи з мети роботи, виникають наступні завдання: аналіз архітектури *SDN* мережі; аналіз принципу функціонування основних елементів мережі; створення моделі *SDN* мережі на базі протоколу *OpenFlow*; розгортання та конфігурування сегменту *SDN* мережі; розгортання та конфігурування *SDN* контролеру.

Виклад основного матеріалу. Оптимальний розподіл інформаційних потоків вимагає нових підходів до управління мережевою інфраструктурою із-за великої різноманітності мережевих протоколів, як для передачі трафіку так і для вирішення завдань керування мережевими ресурсами. Це пов'язано, з існуванням великої кількості різноманітних комунікаційних технологій, як правило препроарітарних та несумісних, з іншого боку – існуюче мережеве обладнання різних фірм виробників не має стандартизованих програмних інтересів, що не дозволяє реалізувати багатокритеріальне та «багаторівневе» управління в складних гетерогенних структурах. Одним їх напрямів „модернізації” класичного підходу щодо організації мережевої архітектури є створення програмно-конфігурованих мереж (*SDN*), що використовують протокол *OpenFlow*. Розробкою стандарту керував альянс *ONF (Open Networking Foundation)*. Поточна версія протоколу 1.5.1 (*OpenFlow 1.6* 2016 року доступний лише для членів *ONF*). До основних переваг мереж *SDN* відносять: централізоване управління в мультівендорному середовищі; зменшення складності керування мережі за рахунок автоматизації; висока швидкість впровадження інновацій; збільшення надійності та безпеки мережі; забезпечення узгодженості політик управління доступом; інжиніринг трафіку; поліпшення якості надання послуг користувачам.

Існує два типи контролерів *SDN*: контролери *SDN* для віртуалізації мережевих функцій *NFV (Network Function Virtualization)* центру обробки даних; та контролери *SDN* для управління *OpenFlow* комутаторами мережі. У випадку віртуалізації інфраструктури (*NFV*) ЦОД, контролери в основному розроблені для забезпечення централізованого управління мережевим рівнем *Openstack Neutron* між віртуальними портами створеними *Nova*. Технологія контролерів *SDN* полягає в управлінні функціями ядра *Unix*, що складаються з *IP*-маршрутизації *L3*, мостів *Unix* та *Open vSwitch*. При цьому інтерфейси між площинами стандартизовані, щоб забезпечити сумісність обладнання в різних областях мережі оператора. **Висновки.** В роботі планується детально розглянути процес міжмережевого обміну між елементами *SDN* мережі на базі протоколу *OpenFlow*. Для цього пропонується створити віртуальний сегмент *SDN* мережі та провести його конфігурування. При чому, топологія мережі буде розгорнута в емуляторі *Mininet* за допомогою скрипта на мові програмування *Python*, також буде розгорнутий зовнішній *HPE VAN SDN controller* який має зручний *web* інтерфейс для контролю та отримання статистичних даних.

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ВИЯВЛЕННЯ СЕРВІСІВ ДЛЯ БАЛАНСУВАННЯ *HIGH-LOAD* СИСТЕМ НА ОСНОВІ ТЕХНОЛОГІЇ *DOCKER SWARM*

Актуальність. Широке використання хмарних сервісів для розгортання *high-load* систем обумовлене застосуванням методів балансування навантаження, що забезпечує: підвищення загальної продуктивності та використання обчислювальних ресурсів; гнучке управління системою; покращення якості надання сервісів; оптимізацію споживання електроенергії, стабільність та ефективність роботи корпоративних інфокомунікаційних систем. Дані технології перспективні та можуть бути використані для побудови ЦОД Міністерства оборони України. Необхідно відмітити, що балансування навантаження на основі технології *docker swarm* також забезпечує кращу відмовостійкість та збільшує термін служби серверного обладнання, завдяки рівномірному розподілу вхідних запитів користувачів.

Постановка проблеми. Проблеми недостатньої продуктивності *high-load* систем в зв'язку зі зростанням вхідного навантаження можна вирішувати шляхом нарощування потужності системи або оптимізації (комбінування) алгоритмів балансування за рахунок завантаженості. При чому збої в роботі серверу (або сервісу) можуть призвести до негативних наслідків, що недопустимо для військових систем, так як вони є об'єктами критичної інфраструктури.

Мета дослідження. Зважаючи на окреслену проблему, основною метою є визначення особливостей, переваг та недоліків використання *high-load* систем у процесі побудови мікросервісів, способів використання технології *docker swarm*, розробки програмного забезпечення щодо комбінованого балансування навантаження між вузлами кластера та його інтеграції в розгорнутий віртуальний сегмент.

Виклад основного матеріалу. Для досягнення поставленої мети і вирішення проблемних питань існують наступні рішення – використання мікросервісів та технологій балансування контейнерів після інкапсуляції та конфігурування кожного сервісу.

Docker – програмне забезпечення з відкритим вихідним кодом, що застосовується для розробки, тестування, доставки і запуску веб-додатків у середовищах з підтримкою контейнеризації. Він потрібен для ефективного використання систем і ресурсів, швидкого розгортання готових програмних продуктів, а також для їх масштабування і перенесення в інші середовища з гарантованим збереженням стабільної роботи. Основними перевагами використання цієї технології є зменшення часу запуску; швидке розгортання програмного забезпечення; зручне керування та масштабування контейнерів; використання обчислювальних ресурсів; підтримка різних операційних систем.

В свою чергу *Docker Swarm* – це власна система оркестрування контейнерів *Docker*, яка використовує стандартний *API Docker* та мережу, що дозволяє легко потрапляти в середовище безпосередньої роботи з контейнерами.

Основні можливості *Docker Swarm*:

- управління навантаженням (здійснює оптимізацію розсилки запитів між хостами);
- динамічне управління (допускає додавання елементів у *swarm*-кластер без подальшого його перезапуску);
- можливість масштабування (дозволяє додавати або видаляти *docker*-образ для автоматичного створення контейнера);
- відновлення «вузла» після збою;
- *rolling-update* (виконує оновлення контейнерів).

Процедура балансування може здійснюватися за допомогою наступних алгоритмів:

1. Алгоритм *Round Robin* або алгоритм кругового обслуговування – це алгоритм, який забезпечує розподіл навантаження обчислювальної системи і використовує впорядкування її

елементів по круговому циклу. Однією з переваг *Round Robin* є вирішення проблеми переходу процесу у стан очікування на невизначений термін під час якого здійснюється раціональний розподіл ресурсів процесора.

Метод *Round Robin* має наступні недоліки: чим вище квант часу, тим вище час відгуку в системі; чим менше квант часу, тим вище витрати на перемикання контексту в системі; вибір оптимального кванту часу є складним завданням в процесі конфігурування системи.

2. Алгоритм *Weighted Round Robin* – це алгоритм планування, який використовується в мережах для направлення потоків даних та процесів, послідовного розподілу запитів у пулі реальних серверів і їх завантаження з більшою продуктивністю. За рахунок даного алгоритму можливо надавати більше навантаження для черг з дрібними пакетами даних.

3. Алгоритм *Least Connections* – спосіб врахування кількості з'єднань, які встановлено з кожним сервером бекенд-пулу та передача нового з'єднання на сервер з найменшою кількістю активних клієнтів. При цьому використовується припущення, що кожне з'єднання генерує однакове навантаження на сервер. Переваги *Least connections*: підходить для задач, пов'язаних з довготривалими з'єднаннями (наприклад, для розподілу навантаження між серверами БД). Тобто, якщо на певних вузлах буде занадто багато активних підключень – нових запитів вони вже не отримають і навпаки. Недоліками даного алгоритму є відсутність сенсу застосовувати алгоритм для задач з короткими сесіями (наприклад для *http* протоколу).

4. Алгоритм *Destination Hash Scheduling* – алгоритм планування хешування джерела, що призначає мережеві підключення до серверів шляхом пошуку статично призначеної *hash* -таблиці за їх *IP*-адресами джерела. До того ж важливим є і розподіл запитів у пулі реальних серверів відповідно до *IP* одержувача на основі статичної *hash*-таблиці. Цей алгоритм реалізується для роботи з кластером хешування проксі-серверів.

5. Алгоритм *Sticky Sessions* – під час використання цього методу запити розподіляються по серверам на основі *IP*-адрес клієнта. Як ключ для хешування використовуються перші три октети *IPv4*-адреса клієнта або *IPv6*-адреса клієнта повністю. Метод гарантує, що запити одного і того ж клієнта будуть завжди передаватися на один і той самий сервер. Якщо ж цей сервер буде вважатися недоступним, то запити цього клієнта будуть передаватися на інший.

Даний метод балансування має певні мінуси, а саме: проблеми з підтримкою сесії при використанні клієнтом динамічної *IP*-адреси; якщо велика кількість запитів проходить через один проксі сервер, то можливе нерівноправне розділення навантаження, але використання *cookie* вирішує ці проблеми. Основними перевагами *Sticky Sessions* є досить просте впровадження для досвідчених адміністраторів мережі; зменшення потреби в реалізації відмови сеансу, оскільки користувачі можуть переходити на інші сервери, лише якщо один з них у автономному режимі; здатність швидкого переходу між запитами, ніж в балансувальника на основі *DNS*. У процесі переходу серверу в автономний режим - сеанс роботи усіх користувачів завершується.

Висновки. За результатами проведеного аналізу було розгорнуто віртуальний стенд, що дозволяє використовувати *Docker Swarm* для управління кластером контейнерів. В подальшому планується провести дослідження ефективності сегменту *high-load* системи при комбінування розглянутих алгоритмів балансування у різних умовах експлуатації.

ЛІТЕРАТУРА

1. Khorov E. Radio Resource Scheduling for Low-Latency Communications in LTE and beyond / E. Khorov, A. Krasilov, A. Malyshev – IEEE/ACM International Symposium on Quality of Service. – 2017. – 6 pp. DOI: 10.1109/IWQoS.2017.7969162.
2. Klyuchnik, S. V. (2018). On the issue of load capacity of old span structures. Bridges and tunnels: theory, research, practice: coll. Science. etc. DNUZT them. acad. Lazaryan, Dnepropetrovsk, 13, 12 – 24.

ПІДСИСТЕМА ОПТИМІЗАЦІЇ ETL ПРОЦЕСІВ НА ОСНОВІ АЛГОРИТМУ КЛАСТЕРИЗАЦІЇ *k-means* КОМПЛЕКСУ СПЕЦІАЛІЗОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ „ПЛАТФОРМА НИЗОВОГО МОНІТОРИНГУ ОБ’ЄКТІВ БУДІВНИЦТВА МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ „*GROUND CONTROL*”

Актуальність обумовлена стрімким розвитком оборонного сектору України, який призвів до суттєвого збільшення кількості обсягів даних, які мають оброблятися відповідними підрозділами. Для вирішення цієї проблеми керівництвом МОУ було визначено одним з пріоритетних напрямків реформи ЗСУ на 2020-2025 роки – розвиток військової інфраструктури та переведення її обліку в електронний формат.

Мета дослідження полягає у вдосконаленні механізму обліку об’єктів нерухомого майна МОУ, переведенні його в електронний формат за рахунок виконання **наступних часткових завдань дослідження**: проаналізувати особливості обліку робіт, що проводяться над нерухомим майном МОУ; дослідити методи агрегації, кластеризації та способи обробки даних; розробити програмний модуль агрегації та обробки даних комплексу СПЗ „Платформа низового моніторингу об’єктів будівництва Міністерства оборони України „*Ground Control*” (далі СПЗ „*Ground Control*”); розробка архітектури та структури підсистеми автоматичної обробки та трансформації даних між елементами СПЗ.

Виклад основного матеріалу. На сьогоднішній день в ЗСУ є проблема майже повної відсутності автоматизації процесів обліку процесів логістики, особливо обліку нерухомого майна. Виходячи з даних проблем, була поставлена оперативна задача створити комплекс СПЗ „*Ground control*”. Це програмне забезпечення, призначене для організації процедури моніторингу стану готовності об’єктів житлового та нежитлового фонду МОУ на основі встановлених керівними документами експлуатаційно–технічних показників; проведення експертної інформаційно–аналітичної оцінки стану готовності об’єктів житлового та нежитлового фонду МОУ з подальшим прогнозуванням планів здачі даних об’єктів в експлуатацію.

Для розробки підсистеми оптимізації *ETL* процесів буде використано метод кластеризації, зокрема метод *k-means*. Метод *k-means* – це ітеративна процедура, яка ділить задану сукупність елементів на *k* кластерів, точки яких є максимально наближеними до їх центрів, а сама кластеризація відбувається за рахунок зміщення цих центрів. Метод прагне мінімізувати сумарне квадратичне відхилення точок кластерів від центрів цих кластерів (критерій ефективності). Основним інструментом для проведення кластеризації, було обрано інструментарій з відкритих вихідним кодом – *Apache Spark*. *Apache Spark* – є інструментом екосистеми *Apache Foundation*, та широко використовується компаніями для аналітики *BigData*. Вбудований інструментарій дає змогу конвертувати дані про агреговані звіти, про стан об’єктів будівництва, для кластеризації їх по заданій кількості категорій з використанням алгоритму *k-середніх*.

Висновки. Отже задача агрегації та управління ускладнюється складною моделлю даних та її неоднорідністю. Спираючись на вимоги поставлені до задачі про агрегацію великої кількості різнорідних типів даних є необхідність використання найпоширеніших типів звітних документів, та створення алгоритму їх обробки. Побудова алгоритму обробки базуватиметься на основі побудови єдиної узагальненої моделі з динамічною кількістю завчасно відомих полів. Поділ і класифікація документів відбуватиметься на основі алгоритму кластеризації *k-means*. Для обробки файлів великого обсягу найкраще підходить потокова обробка за допомогою інструментів розподілених файлоховищ, таких як *Hadoop*, та розподілених систем обчислення таких, як *Apache Spark*.

ПІДСИСТЕМА ОЦІНКИ ПРОДУКТИВНОСТІ ІР РВХ ПРИ ВИКОРИСТАННІ РІЗНИХ ТИПІВ ВІРТУАЛІЗАЦІЇ

Актуальність. На даному етапі розвитку обчислювальних мереж все більш широко використовується перехід від горизонтального до вертикального масштабування. Одним із аспектів цього принципу є зменшення кількості фізичних серверів, які замінюються їх віртуальними аналогами. У зв'язку з цим, технологія віртуалізації фізичного обладнання відіграє ключову роль в питаннях побудови інформаційно-телекомунікаційних мереж. Суть технології віртуалізації полягає в можливості розміщення декількох ізольованих середовищ на одному фізичному сервері, що дозволяє зменшити кількість фізичного обладнання і заощадити витрати на серверне та мережеве обладнання для Збройних Сил України. На сьогоднішній день є доцільним використовувати технології віртуалізації в корпоративних мережах. При цьому слід врахувати такі параметри, як швидкодія віртуального середовища, навантаження на систему, простота розгортання, тощо.

Мета дослідження полягає у визначенні продуктивності роботи мережевих служб при використанні основних типів сучасних технологій віртуалізації. А саме, проведення аналізу використання віртуальних машин та віртуальних контейнерів для розгортання ІР АТС, при різних режимах функціонування.

Виклад основного матеріалу. Віртуалізація мереж та систем була в центрі уваги багатьох провідних організацій в галузі інформаційних технологій досить довгий період часу. Основною метою технологій віртуалізації є консолідація серверів або центрів обробки даних, зниження капітальних витрат, зменшення витрат на фізичне обладнання побудови мережі. Найбільш поширеними технологіями віртуалізації є віртуалізація на основі віртуальних машини та контейнерна віртуалізація. Віртуальні машини здійснюють віртуалізацію за рахунок гіпервізора, який встановлюється поверх операційної системи або поверх фізичного сервера. Віртуальні машини забезпечують повну ізоляцію від інших, що працюють на одному фізичному сервері. В свою чергу контейнери вважаються більш ефективними в плані використання наявних ресурсів, ніж віртуальні машини, оскільки усувається необхідність в застосуванні додаткових ресурсів для кожної операційної системи. Тобто, один фізичний (віртуальний) сервер може розміщувати більше *docker*-контейнерів в порівнянні з віртуальними машинами. Що в свою чергу, впливає на продуктивність затрачених ресурсів під час роботи мережевих служб, а саме економія використання фізичних ресурсів. Однією із перспективних технологій, яка набула широкого використання, являється *VoIP* телефонія. В зв'язку з цим постає завдання оцінки показників функціонування програмного рішення *IP PBX (Private Branch eXchange) Asterisk* з використанням технології віртуальних машин та контейнерів. Для цього був розгорнутий віртуальний сегмент *VoIP* телефонії та за допомогою вбудованих засобів моніторингу та утиліти *Scots realtime* в реальному масштабі часу були зняті показники використаних ресурсів ІР АТС. Результати показують, що впровадження технологій віртуалізації дозволяє підвищити ефективність використання серверного обладнання, а також надійність та безвідмовність надання інформаційних послуг.

Висновки. Досліджено сучасні методи віртуалізації, що використовуються для покращення функціонування серверів та підвищення ефективності серверних ресурсів при побудові сегменту *VoIP* телефонії на базі *IP PBX Elastix*. Для оцінки функціонування було розгорнуто підсистему оцінки продуктивності *IP PBX* на основі віртуального та фізичного серверів з використанням різних типів віртуалізації, а саме гіпервізора *ESXi* та віртуальних контейнерів *Docker*. В подальшому планується проведення оцінки продуктивності мережевих служб при застосуванні кластеризації серверів на основі контейнерів та віртуальних машин.

ПІДХОДИ ЩОДО ВИБОРУ І НАЛАШТУВАННЯ СЕРВОПРИВОДІВ ДЛЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ КЛАСУ 1 З УРАХУВАННЯМ ПОТРЕБ І ДОСВІДУ ОПЕРАЦІЇ ОБ'ЄДНАНИХ СИЛ

Швидкий розвиток набуває озброєння з використанням роботизованих систем, якими можна вважати безпілотні літальні апарати (БпЛА) для ведення повітряної розвідки. Усі передові держави світу озброєні БпЛА різних видів та класів. Даний вид озброєння виконує майже всі завдання по веденню бойових дій на дистанціях без загрози життю і здоров'ю людини. БпЛА – це зброя яка набуває великих обертів у розвитку. Вже сьогодні існують „рої” дронів, які з легкістю можуть знищити особовий склад від відділення до роти і навпаки вміє і своєчасне їх використання дозволе випередити противника і зберегти життя свого особового складу.

Особливої уваги слід приділити виконавчим механізмам (сервоприводам) їх перевірку та налаштування БпЛА, які забезпечують основну роботу літального апарату. Сервопривод – це пристрій, який за допомогою енергії здійснює механічне переміщення регулюючого органу, відповідно до отримуваних від системи команд. Сервоприводи поділяються на аналогові (містять спеціальну мікросхему) та цифрові (містять мікропроцесор, який приймає і аналізує імпульси). Перевагу мають цифрові так, як вони більш функціональні, але в рази дорожчі за аналогові. Сервоприводи відповідають за роботу аеродинамічних органів керування, та цільової апаратури, а також парашутних відсіків, які забезпечують залежно від виду БпЛА, як основну так і аварійну посадку.

Налаштовуються сервоприводи за допомогою програмного забезпечення, де програмується кут повороту сервоприводу та час спрацювання. Одна із найпоширеніших причин поломок сервоприводів це – не правильно розраховані параметри (кг/см), а також матеріал з якого зроблено відхиляючий механізм. Запобігти надмірним динамічним навантаженням на сервомеханізм можливо, за допомогою плавного розгону, або ж такого плавного гальмування. Масово БпЛА почали використовувати з початком бойових дій на сході України, де оператори та пілоти зіштовхнулись з несправностями сервоприводів, які призводили до падіння БпЛА і його пошкодження. Це відбувається, як при взльоті так і при посадці, коли сервоприводи виходять із роботи і аеродинамічні органи не відповідають на команди пілота чи оператора. Але найбільша проблема – це коли сервомеханізм не виконує свою роботу за призначенням, вже набравши висоту і виконуючи місію на відстані від точки взльоту. Через таку несправність екіпаж не виконує поставлене завдання, а БпЛА найчастіше втрачається, або призводить до падіння.

Для успішного виконання завдань та не допущення падіння, через несправності сервоприводів, потрібно їм приділяти особливу увагу під час проведення передполітної перевірки та підготовки. Своєчасно здійснювати заміну сервоприводів та відхиляючого механізму. Правильно підбирати розміри сервомеханізмів відповідно до навантажень роботи за співвідношенням (кг/см). Перевірити правильність роботи сервоприводу, відповідно до поданої команди та час його спрацювання.

Все це можна вирішити шляхом розробки пристрою який перевірятиме справність сервоприводів на виконання ними роботи заданої при первинних налаштуваннях та програмуванні механізму. Ефективність застосування запропонованого підходу буде найвищою, при автоматичному виведенні відповідної інформації на наземну станцію управління БпЛА із урахуванням градації допустимих норм працездатності (використання сервоприводу).

МЕТОДИКА ВИБОРУ ЗНАЧЕНЬ ПАРАМЕТРІВ СИГНАЛІВ З ППРЧ В УМОВАХ РАДІОЕЛЕКТРОННОГО ПОДАВЛЕННЯ

Як показує аналіз основних методів підвищення завадозахищеності систем і засобів радіозв'язку ефективним напрямком протидії радіотехнічній розвідці та радіоелектронному подавленню (РЕП) є застосування в сучасних засобах радіозв'язку (ЗРЗ) режиму псевдовипадкового перестроювання робочої частоти (ППРЧ).

При побудові засобів радіозв'язку з ППРЧ велика увага приділяється питанням оптимізації алгоритмів формування та обробки сигналів, які дозволяють підвищити якість функціонування при заданих обмеженнях на інші показники.

На даний час питання ефективності функціонування засобів радіозв'язку з ППРЧ досить глибоко й широко досліджені в наукових працях вітчизняних та іноземних авторів. Але більшість відомих методів підвищення ефективності ЗРЗ орієнтовані на канали при середніх відношеннях енергії сигналу до спектральної щільності потужності завади, що не повною мірою відповідає завадовій обстановці в реальних каналах зв'язку при дії засобів радіоелектронної боротьби. Крім того, існуючі методи управління параметрами сигналів засобів радіозв'язку орієнтовані в основному на статичні або квазістатичні умови їх функціонування і не можуть бути застосовані в умовах складної радіоелектронної обстановки при впливі комплексу навмисних завад, які створює система РЕП.

Отже, завдання підвищення енергетичної ефективності засобів радіозв'язку в умовах активної радіоелектронної боротьби є актуальним і має не тільки теоретичне, але і велике прикладне значення для забезпечення необхідного рівня бойової готовності військ за рахунок підвищення своєчасності, вірогідності та прихованості бойового управління.

У доповіді запропоновано методику вибору значень параметрів сигналів з ППРЧ, сутність якої полягає у адаптивному виборі значень параметрів сигналу засобів радіозв'язку з ППРЧ військового призначення, оптимальних за критерієм максимуму показника енергетичної ефективності при обмеженнях на ймовірність помилкового приймання в залежності від завадової обстановки в каналі зв'язку. Процес визначення оптимальних значень параметрів сигналу з ППРЧ складається з наступних етапів:

1) оцінка стану каналу. На даному етапі, оцінюються просторові параметри джерел радіовипромінювань з псевдовипадковим перестроюванням робочої частоти. Крім того, для конкретного радіозасобу визначаються вид і характеристики навмисних завад, які діють на вході приймача;

2) вибір параметрів сигналу. В залежності від виду завади, яка діє на вході приймача, вибирається позиційність ансамблю сигналів, швидкість перестроювання частоти та величина коефіцієнта розширення спектра сигналу;

3) вибір коригувального коду;

4) вибір маніпуляційного коду для узгодження характеристик кодека двійкового завадостійкого коду і модема багатопозиційних сигналів.

5) перевірка виконання вимог по забезпеченню завадостійкості приймання сигналів.

У переважній більшості випадків виявляється можливим виділити декілька можливих сценаріїв завадової обстановки. Цим сценарієм у відповідність можуть бути поставлені N різних сигнально-кодових конструкцій, які доцільно вибирати виходячи з параметрів ефективності засобів радіозв'язку при впливі різних видів навмисних завад.

Дослідження розробленого алгоритму функціонування адаптивної системи радіозв'язку за розробленою методикою показало, що адаптивна схема побудови засобів радіозв'язку забезпечує в середньому на 16-27 % більш високу енергетичну ефективність (коефіцієнт використання потужності сигналу), ніж не адаптивна.

ДИНАМІЧНА МОДЕЛЬ РАДІОЕЛЕКТРОННОГО КОНФЛІКТУ З УРАХУВАННЯМ МОЖЛИВОСТЕЙ СТОРІН

Удосконалення засобів і комплексів навмисного деструктивного впливу на інформаційні системи вимагає розвитку науково-методичного апарату моделювання ефективності таких впливів.

На даний час недостатньо вивченими є динамічні та перехідні процеси розвитку радіоелектронних конфліктів. Крім того, в низці опублікованих робіт вказується на те, що в ході конфлікту існує можливість в реальному масштабі часу захоплювати і перерозподіляти радіо ресурс на свою користь. Однак зазначені процеси також є недостатньо дослідженими.

З огляду на це, аналіз динамічних процесів при розвитку конфлікту радіо систем з урахуванням їх можливостей зі спостереження, захоплення і блокування радіо ресурсу противника є актуальним напрямком досліджень.

Метою роботи є розроблення динамічної моделі радіоелектронного конфлікту з урахуванням можливостей сторін зі спостереження, захоплення і блокування радіо ресурсу противника. При цьому в якості конфліктуючих систем виступають інтегровані системи, що мають у своєму складі підсистему спостереження, підсистему захоплення і блокування радіо ресурсу системи противника, а також власну радіо підсистему, яка захищається від зовнішнього впливу.

В основу підходів до побудови моделі були покладені відомі дослідження з теорії популяційної динаміки, які моделюють конкуренцію і боротьбу різних біологічних видів у процесі їх еволюції, а саме: нейро-нечіткі нейронні мережі, що еволюціонують; генетичні алгоритми та алгоритми мурашиних колоній.

Для побудови математичної моделі радіоелектронного конфлікту та її дослідження був використаний математичний апарат теорії динамічних систем. Сама модель представлена у вигляді системи чотирьох нелінійних диференціальних рівнянь.

Новизною моделі є врахування в ній динаміки розвитку радіоелектронного конфлікту, а також можливостей сторін зі спостереження, захоплення і блокування радіо ресурсу.

Підсумками дослідження моделі є виявлені типові стани конфлікту, а також біфуркації конфлікту – такі значення параметрів конфліктуючих сторін, за яких якісно змінюються траєкторії розвитку конфлікту і можливості виграшу тієї чи іншої сторони. На основі цих досліджень були запропоновані сценарії дій однієї зі сторін щодо зміни її параметрів для досягнення виграшу в конфлікті.

Проведено детальний аналіз типових сценаріїв дій для однієї зі сторін, в інтересах обґрунтування найбільш „сильних” параметрів і напрямків їх зміни для забезпечення виграшу.

Практична значимість представленої моделі радіоелектронного конфлікту полягає в тому, що вона може бути використана для дослідження широкого класу антагоністично-конфліктних взаємодій інформаційно-технічних систем у таких прикладних галузях, як радіоелектронна боротьба, радіо- і радіотехнічний моніторинг, а також радіоелектронне протиборство в технічній сфері.

Представлені в роботі сценарії можуть бути використані для вдосконалення математичного забезпечення відповідних технічних комплексів в інтересах забезпечення їх переваги в подібних динамічних конфліктах.

Напрямки подальших досліджень доцільно спрямувати на розроблення методологічних основ підвищення стійкості систем спеціального призначення, що функціонують в умовах активного радіоелектронного подавлення.

ВІДОМІ АТАКИ НА СХЕМУ ЦИФРОВОГО ПІДПISY FALCON

На сьогодні питання знаходження стійкого алгоритму направленого шифрування для постквантового періоду залишається актуальним. Це пов'язано в першу чергу з розвитком технологій, а саме з побудовою квантового комп'ютера. Як відомо, декілька років тому NIST оголосив про конкурс стандартизації одного чи декількох квантово-стійких алгоритмів шифрування з відкритим ключем та цифрових підписів, ідеєю якого є знаходження алгоритму шифрування та цифрового підпису, який би був стійким до квантових атак. Наразі NIST проводить третій раунд конкурсу NIST PQC, на якому фіналістами стали лише 7 кандидатів [1-6]. Серед них 4 алгоритми шифрування з відкритим ключем та алгоритми встановлення ключа, та 3 алгоритми цифрового підпису. Метою доповіді є розгляд схеми цифрового підпису (ЦП) Falcon, чия безпека базується на складності пошуку коротких векторів на решітці, а також атаки на даний алгоритм.

Falcon – це схема підписів, що має в основі решето числового поля, що використовує парадигму «гешуй і підписуй». Безпека базується на складності проблеми SIS (коротке ціле рішення) над решітками NTRU, а докази безпеки наводяться як у випадковій моделі оракула (ROM), так і в QROM із жорсткими скороченнями. Falcon є більш складним у реалізації, ніж Dilithium, вимагаючи деревоподібних структур даних, великих операцій з плаваючою точкою та випадкової вибірки з кількох дискретних розподілів Гауса [2].

Однією з переваг Falcon є те, що він пропонує найменшу пропускну здатність (розмір відкритого ключа та розмір підпису) з усіх схем цифрового підпису третього раунду. Falcon також ефективний у підписанні та верифікації, хоча генерація ключів відбувається повільніше. Falcon можна легко застосувати до існуючих протоколів та додатків і він забезпечує дуже хорошу загальну продуктивність. Розглянемо відомі атаки на схему Falcon.

Відновлення ключа. Найефективніші атаки походять від редукції решітки. Почнемо з розгляду решітки, породженої стовпцями $\begin{bmatrix} q & h \\ 0 & 1 \end{bmatrix}$. Після використання редукції решітки на цій основі ми перераховуємо всі точки решітки в колі радіусом $\sqrt{2n} \cdot \sigma_{\{f,g\}}$, з центром на початку координат. Тому ми маємо значну ймовірність знайти $\begin{bmatrix} g & f \end{bmatrix}$.

Нехай λ буде $(2n-B)$ -а норма Грама-Шмідта, яка є приблизною нормою найкоротшого вектора решітки, породженої останніми векторами B , розташованими ортогонально першим $2n-B-1$ векторам. Алгоритм решета, виконаний на цій проектованій решітці, відновить усі вектори норми, менші за $\sqrt{4/3}\lambda$. Якщо серед них є проекція ключа, саме тоді

$$\sqrt{B}\sigma_{\{f,g\}} \leq \sqrt{4/3}\lambda,$$

ми можемо з великою ймовірністю відновити вектор секретного ключа з його проекції, використовуючи алгоритм найближчої площини Бабаї на всіх відібраних векторах. Це пояснюється тим, що всі інші норми Грама-Шмідта більші за λ , що набагато більше, ніж $\sigma_{\{f,g\}}$.

Для найвідомішого алгоритму редукції решітки DBKZ [5, 2], отримаємо:

$$\lambda = \left(\frac{B}{2\pi e} \right)^{1-n/B} \sqrt{q}, \text{ та } (B/2\pi e)^{1-n/B} \sqrt{q} = \sqrt{3/4} B \sigma_{\{f,g\}}.$$

Підробка підпису. Підробка підпису може бути виконана шляхом знаходження точки решітки на відстані, обмеженої β від випадкової точки, в тій самій решітці, що і вище. Це

завдання також можна вирішити за допомогою редукції решітки. Один з можливих варіантів полягає у використанні вбудовування Каннана, тобто додавання $(H(r\|m), 0, K)$ до базису решітки, розширеного на ряд нулів, що дає наступну матрицю:

$$\begin{bmatrix} q & h & H(r\|m) \\ 0 & 1 & 0 \\ 0 & 0 & K \end{bmatrix}.$$

Оскільки алгоритми решета генерують безліч коротких векторів, ми, безперечно, можемо знайти серед них вектор виду $(c, *, K)$ і тоді $H(r\|m) - c$ є точкою решітки.

Беручи $K \approx \sqrt{q}$, алгоритм DBKZ [5, 2] дає успішні умови для підробки:

$$\left(\frac{B}{2\pi e}\right)^{n/B} \sqrt{q} \leq \beta.$$

Це найкраща атака проти Falcon. Необхідно перетворити розмір блоку B у конкретний бітово-безпечний, дотримуючись методології New Hope [6], яку іноді називають „методологією core-SVP”.

Також було розглянуто *гібридну атаку*, що поєднує в собі алгоритм зустрічі посередині та алгоритм відновлення ключів, та *алгебраїчні атаки*, але їх вплив на Falcon не дуже ефективний та значний [1-6].

1. Під час третього раунду NIST заохочує до більш детального вивчення реалізації Falcon, щоб визначити, чи робить арифметика з плаваючою крапкою помилки реалізації більш імовірною, ніж інші схеми, чи забезпечує шлях для атак бічними каналами.

2. Найефективніші атаки походять від редукції решітки. Найкращою атакою на даний момент часу є підробка підпису.

3. Гібридна атака та алгебраїчні атаки не мають значного впливу на Falcon. Однак існують ефективні алгоритми пошуку не дуже малих елементів в ідеалах $\square[x]/(\phi)$ і це потребує більш детального дослідження.

4. Як і у деяких інших кандидатів, параметри рівня I Falcon мають відносно низький рівень безпеки CoreSVP, тому необхідні подальші дослідження.

ЛІТЕРАТУРА

1. Post-Quantum Cryptography Standardization, 2020. [Електронний ресурс]. – Режим доступу: <https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions>.
2. Pierre-Alain Fouque Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU / Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Prest, Thomas Ricosset, William Whyte, Zhenfei Zhang, et al. // Specification v1.2 – 01/10/2020. pp.17, 21-25, 51. 2020.
3. NIST. Submission requirements and evaluation criteria for the post-quantum cryptography standardization process, 2016. [Електронний ресурс]. – Режим доступу: <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography>.
4. Léo Ducas Efficient identity-based encryption over NTRU lattices / Léo Ducas, Vadim Lyubashevsky, Thomas Prest // In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014, Part II*, volume 8874 of LNCS, pages 22 – 41, Kaoshiung, Taiwan, R.O.C., December 7 – 11, 2014. Springer, Heidelberg, Germany.
5. Daniele Micciancio Practical, predictable lattice basis reduction / Daniele Micciancio, Michael Walter // In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of LNCS, pages 820–849, Vienna, Austria, May 8–12, 2016. Springer, Heidelberg, Germany.
6. Erdem Alkim Post-quantum key exchange – A new hope / Erdem Alkim, Léo Ducas, Thomas Pöppelmann, Peter Schwabe // In Thorsten Holz and Stefan Savage, editors, *USENIX Security 2016*, pages 327 – 343, Austin, TX, USA, August 10 – 12, 2016. USENIX Association.

ПІДВИЩЕННЯ СТАЛОСТІ ФУНКЦІОНУВАННЯ МЕРЕЖІ ЦИФРОВОГО ТРАНКІНГОВОГО ЗВ'ЯЗКУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ ШЛЯХОМ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ CAPACITY PLUS MULTI-SITE

Актуальність. На сучасному етапі функціонування мереж цифрового транкінгового зв'язку на базі платформи MOTOTRBO зоні проведення ООС значно зріс попит на телекомунікаційні послуги та чітко просліджується тенденція швидкого зростання об'ємів як голосового трафіку, так і трафіку даних в цих мережах, що вимагає створення телекомунікаційної мережі цифрового транкінгового зв'язку з високою пропускнуою здатністю на базі новітніх технологій.

Постановка задачі. Необхідність створення мережі цифрового транкінгового зв'язку з високою пропускнуою здатністю на базі новітніх технологій для максимального задоволення потреб в послугах мобільного транкінгового зв'язку Міністерства оборони України, Генерального штабу Збройних Сил України, окремих силових структур на державному рівні і рівні окремих користувачів, у тому числі забезпечення оптимізації взаємодії військових формувань Збройних Сил України на всіх ланках управління в зоні проведення операції Об'єднаних сил (ООС).

Мета. Запропонувати варіант технічної реалізації мережі цифрового транкінгового зв'язку спеціального призначення платформи MOTOTRBO на базі нової технології Capacity Plus Multi-Site.

Основні положення. Мережа цифрового транкінгового зв'язку спеціального призначення платформи MOTOTRBO на базі нової технології Capacity Plus Multi-Site має низку переваг, а саме:

- забезпечення інформаційного обміну в мережі транкінгового зв'язку між абонентами пунктів управління при розосередженому розташуванні пунктів управління;
- забезпечення бездротового доступу абонентів пунктів управління до транспортної телекомунікаційної мережі ЗСУ;
- резервування дротової мережі доступу, нарощування телекомунікаційної мережі ЗСУ;
- забезпечення свободи локальних дій окремих груп користувачів у часі та просторі;
- гнучкість інформаційного обміну та можливість адаптації в умовах, що постійно змінюються;
- можливість поєднання локального інформаційного обміну (в підрозділах типової групи користувачів) з глобальними (для Генерального штабу ЗСУ в цілому або між штабом ООС ЗСУ і оперативними секторами і т.і.);
- скорочення потоків інформації, що пропускається через кожний рівень управління;
- високу надійність;
- можливість закриття інформації (шифрування) за допомогою національних апаратно-програмних комплексів та алгоритмів;
- надання послуг в реальному масштабі часу;
- спряження з іншими інформаційними мережами і системами зв'язку з забезпеченням вимог до підключення і якості послуг, що надаються у відповідності з діючою нормативно-правовою базою;
- уніфікованість побудови;
- економічну доцільність (максимальне використання наявного телекомунікаційного обладнання для побудови системи транкінгового зв'язку ЗСУ).

В цілому мережа цифрового транкінгового зв'язку спеціального призначення платформи MOTOTRBO на базі нової технології Capacity Plus Multi-Site може мати у своєму складі до 15 сайтів з максимальною кількістю до 12 ретрансляторів на один сайт, а саме: до 8 ретрансляторів (16 розмовних каналів) та до 4 ретрансляторів (8 каналів) передачі даних.

Максимальна кількість обслуговування рухомих абонентів мережі може складати до 1600 на один сайт. В цілому мережа може обслуговувати до 24000 абонентів, які можуть бути згруповані у 255 окремих груп.

Управління такою мережею здійснюється ієрархічним комплексом диспетчеризації з розмежуванням прав доступу. Комплекс диспетчеризації може забезпечити:

організацію зв'язку з трьома типами абонентів – радіостанції MotoTRBO, абоненти IP-телефонії за протоколом SIP, іншими диспетчерськими консолями);

підтримку всіх типів викликів (індивідуальні, групові, загальні);

ідентифікацію абонентів;

вибіркове прослуховування радіостанцій;

екстрені виклики;

голосові виклики між диспетчерами (Intercom);

запис переговорів;

перевірку радіостанції на присутність у мережі;

оповіщення про виклик;

примусове відключення радіостанцій;

гнучке настроювання звуку;

гнучке настроювання вікон виклику абонентів;

дерево категорій для абонентів системи;

використання профілів для обмеження доступу операторів до базових станцій, групам, службам радіомережі, тайм-слотам.

відстеження місць розташування радіостанцій в реальному часі;

підтримку різних типів мап (векторні, растрові, INGIT, MapPoint, Google);

збереження даних про місце розташування абонентів у базі даних;

забезпечення можливості зовнішнього доступу до бази даних розташування абонентів зі сторони спеціалізованого програмного забезпечення;

аналіз треків переміщення абонентів за заданий період часу;

анімацію переміщення абонентів по треку;

деталізацію переміщень до кожної окремої координати;

відстеження входу абонентів у задані зони та виходу з них;

відстеження простою абонентів більше заданого часу;

повідомлення про початок руху;

відстеження втрати та появи координат від абонентів;

відображення на мапі всіх абонентів обраної категорії;

функцію автоматичного одержання місця розташування (інтервал задається для кожного абонента окремо);

функцію одержання місця розташування по події;

функцію одержання місця розташування по запиту (по натисканню кнопки);

функцію вивантаження координат в KML-форматі із заданим інтервалом часу (для відстеження місця розташування в Google Map API та спеціалізованому програмному забезпеченні).

В мережі відсутній загальний контролер системи– технологічне управління системою здійснюється одним із 180 ретрансляторів мережі, який запрограмований як „майстер”.

Висновок. Запропонований варіант побудови мережі цифрового транкінгового зв'язку на базі технології Capacity Plus Multi-Site повністю вирішить проблеми своєчасного забезпечення мобільним транкінговим захищеним зв'язком штабів, військових формувань та інших структур Збройних Сил України в зоні проведення ООС.

СИСТЕМА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ВІЙСЬКОВОЇ ОСВІТИ З ПИТАНЬ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ ВИПУСКНИКІВ ВВНЗ ЗА ПІДСУМКАМИ ЇХ СЛУЖБОВОЇ ДІЯЛЬНОСТІ

Актуальність. Оцінювання професійної діяльності має важливе значення в забезпеченні успішної адаптації молодих офіцерів. Цей процес постійного спостереження, вивчення і оцінювання професійної діяльності за визначеними критеріями результатів його діяльності та прояви якостей являє собою дієвий інструмент виражених кадрових рішень в процесі якісного управління кар'єрою офіцерів. На теперішній час головними джерелами інформації про проходження випускниками служби у військах є звіти науково-педагогічних працівників ВВНЗ та ВВП ЗВО, які проводили військове стажування та анкети-відгуки із військ. Даний звіт не забезпечує розгляд професійної діяльності офіцера-випускника, які визначені у професійному стандарті військового фахівця Збройних Сил України та компетентності. Виходячи з цього є необхідність створення інформаційної системи для забезпечення військової освіти з питань оцінювання результатів навчання випускників ВВНЗ за підсумками їх службової діяльності. **Мета дослідження.** Створення інформаційної системи для забезпечення військової освіти з питань оцінювання результатів навчання випускників ВВНЗ за підсумками їх службової діяльності для можливості розгляду професійних діяльностей офіцера-випускника, які визначені у професійному стандарті військового фахівця Збройних Сил України та визначення конкретних недоліків в підготовці військових фахівців з метою подальшого внесення змін у в навчальні плани та програми навчальних дисциплін для їх покращення. Для досягнення вказаної мети у роботі сформульовано наступні **часткові завдання:** Аналіз існуючих підходів в оцінюванні результатів навчання випускників ВВНЗ та ВВП ЗВО за підсумками службової діяльності. Дослідити нормативно-правові акти з питань оцінювання результатів навчання випускників ВВНЗ та ВВП ЗВО за підсумками службової діяльності. Розробка проекту технічного завдання на створення спеціального програмного забезпечення оцінювання результатів навчання випускників ВВНЗ та ВВП ЗВО за підсумками службової діяльності. Розробка макету спеціального програмного забезпечення оцінювання результатів навчання випускників ВВНЗ та ВВП ЗВО за підсумками службової діяльності. Створення програмного забезпечення на основі попереднього дослідження.

Виклад основного матеріалу. Система інформаційного забезпечення військової освіти з питань оцінювання результатів навчання випускників ВВНЗ за підсумками їх службової діяльності створена з використанням клієнт-серверної архітектури на основі платформи *Node.js*. Система реалізує авторизацію, реєстрацію користувача у систему, розмежування прав користувача для створення відгуку з боку безпосереднього командира та самооцінки офіцера, відображення загальної статистики про середню оцінку офіцерів-випускників за їх службовою діяльністю та статистики конкретних недоліків в підготовці військових фахівців. Можливість генерації та завантаження файл-звіту у яких зазначені усі статистика про загальні оцінки офіцерів-випускників та конкретних недоліків у їх підготовці.

Висновок. Під час створення інформаційної системи було проаналізовано керівні документи, які регламентують оцінювання професійної діяльності молодих офіцерів, розроблені проект технічного завдання та макети спеціального програмного забезпечення, обґрунтовано доцільність створення інформаційної системи забезпечення військової освіти з питань оцінювання результатів навчання випускників ВВНЗ за підсумками їх службової діяльності та недоліків під час підготовки та навчання офіцерів.

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ РАДІОСТАНЦІЙ З ШИРОКОСМУГОВОЮ АДАПТИВНОЮ МЕРЕЖЕВОЮ ФОРМОЮ СИГНАЛУ В ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Розвитку та удосконалюванню систем управління та зв'язку приділяють велику увагу. Підтвердженням тому є щорічні навчання військ зв'язку, основною метою яких є планування та підтвердження оперативної, апаратної та програмної сумісності обладнання зв'язку.

Сьогодні першочерговим питанням яке потребує рішення є створення інформаційно-комунікаційної мережі, яка забезпечить доведення до учасників військових операцій достовірної та повної інформації про обстановку в реальному масштабі часу. Як транспортна основа інформаційно-комунікаційної мережі військовими аналітиками запропоновано використання самоорганізованої мережі (Ad-Hoc мережі). Отже, вирішення проблеми впровадження самоорганізованих мереж зв'язку у тактичній ланці управління є актуальною проблемою сьогодення.

Використовуючи адаптивні мережеві широкосмугові сигнали ANW2 (Adaptive Networking Wideband Waveform) УКХ радіостанція RF-7800M-MP, виробництва компанії „Harris”, забезпечує високошвидкісний режим передачі мережевих даних. Для передачі сигналів ANW2 використовуються інноваційні, інтелектуальні протоколи, які не вимагають наявності в мережі станцій управління – кожна станція автоматично виявляє і приєднується до дозволеної мережі. Утворення самоорганізованої мережі (Ad-Hoc) забезпечує автоматичну і зрозумілу ретрансляцію через будь-яку доступну станцію і самовідновлення, якщо будь-яка станція залишає мережу.

Радіостанція RF-7800M-MP відноситься до класу радіостанцій з SCA (Service Component Architecture) архітектурою, що забезпечує оптимальний перехід до технології з програмованими параметрами радіозв'язку. Вбудовані AES і Citadel режими шифрування з 256-бітовим ключем забезпечують високий рівень безпеки для всіх режимів передачі. Застосування спеціальних сигналів радіопротидії стандарту Quicklook ECCM забезпечує захист вузькосмугових сигналів мовної інформації і даних від ворожого втручання, а застосування SCA архітектури дозволяє завантажувати нові види сигналів, які можуть з'явитися в майбутньому.

Широкосмугова адаптивна мережева форма сигналу ANW2 являє собою широкосмуговий сигнал від 225,000 МГц до 1999,995 МГц в діапазоні UHF і дозволяє здійснювати одночасну високошвидкісну передачу голосу і даних.

Використання станцій з технологією ANW2 надасть ряд ключових рішень для формування радіомереж у тактичній ланці управління Збройних сил України, а саме:

Відсутність інфраструктури. ANW2 не вимагає попередньо сконфігурованих головних вузлів або кластера. Це дозволяє ANW2 формувати кілька мереж і постійно адаптуватися до мінливих умов каналу.

Високий рівень безпеки. Дані ANW2 в радіостанції RF-7800M-MP захищаються з використанням стандарту шифрування інтернет-протоколу High Assurance (HAIPE™). Використовуючи цей інтероперабельний мережевий стандарт, RF-7800M-MP сертифікована NSA для передачі даних найвищих ґрифів секретності.

Зміна умов каналу. Вузли не завжди мають зв'язок прямої видимості до інших станцій. Вузли мережі ANW2 вимірюють і повідомляють ці зміни і автоматично адаптуються, вибираючи відповідні модуляції. Модуляція вибирається за принципом „станція-станція”, щоб вся мережа не організовувала низькопродуктивні з'єднання.

Швидке формування і час самовідновлення. ANW2 використовує протокол даних множинного доступу з тимчасовим поділом (TDMA), який забезпечує передбачувану продуктивність і швидкий час формування та відновлення - зазвичай менше 10 секунд.

Голосове з'єднання. ANW2 включає в себе виділення мовного каналу радіозв'язку (CNR), який працює одночасно, але незалежно, від операції з даними.

Масштабованість. Підсистеми ANW2 підтримують від одного до 30 вузлів з повною функціональністю та до 250 вузлів з обмеженою «гостьовою» функціональністю. Це дозволяє організовувати мережі до 280 вузлів в одній підмережі або радіоканалі. ANW2 також використовує стандартні мережеві протоколи і інтерфейси.

Використовуючи ANW2, радіостанція RF-7800M-MP забезпечує підвищену зв'язність даних для рівня батальйону і нижче, включаючи можливість безпечного відновлення в мережах. Ця можливість також розширюється за рахунок використання радіомодемів з високою пропускною здатністю (HCLOS), супутникових терміналів або прямого підключення до захищеної мережі.

Переваги широкосмугових тактичних комунікацій величезні, вони надають користувачам мереж більш широке та гнучке інформаційне середовище. Вони використовуються інноваційні, інтелектуальні протоколи, які не вимагають наявності в мережі станцій управління. Утворення самоорганізованої мережі забезпечує автоматичну і зрозумілу ретрансляцію через будь-яку доступну станцію і самовідновлення, якщо будь-яка станція залишає мережу.

Володіючи значно збільшеними обчислювальними можливостями, радіостанція RF-7800M-MP є перспективним засобом зв'язку з можливостями постійного оновлення та адаптації до майбутніх нових розробок і відноситься до нового покоління широкосмугових ВЧ радіостанцій, які вирішують завдання зв'язку сьогоденного і завтрашнього дня.

ЛІТЕРАТУРА

1. RF-7800M-MP Multiband networking Radio – Harris Corporation / RF Communications. 2011 [Електронний ресурс] . – Режим доступа: http://rf.harris.com/media/RF-7800M-MP_WEB_tcm26-9182.pdf
2. RF-7800M-MP APPLICATIONS Guide – Harris Corporation / RF Communications. 2010 [Електронний ресурс]. – Режим доступа: http://rf.harris.com/media/RF-7800M_Apps_Handbook_tcm26-12261.pdf
3. Шнепс М.А. От IN к IMS. О российской Системе-112: нерешенные задачи / М.А. Шнепс // Int. Journal of Open Inf. Technologies. – 2014. – Т. 2. – № 1. – С. 1 – 11.
4. Біла книга – 2013. Збройні Сили України. – К.: Міністерство оборони України, 2014. – 76 с.
5. Информационные технологии. Системы, средства связи и управления: Информационно-аналитический сборник / Под ред. С.В. ИONOва, ОАО „Концерн „Созвездие”. – Воронеж, 2012. – № 1. – 166 с.
6. Датагруп – оператор рішень [Електронний ресурс]. – Режим доступа: www.datagroup.ua.
7. Mobile Ad Hoc Networking Revamps Military Communications [Електронний ресурс]. – Режим доступа: <http://www.cotsjournalonline.com/articles/view/102158>.
8. Самоорганизующиеся радиосети со сверхширокополосными сигналами / С.Г. Бунин, А.П. Войтер, М.Е. Ильченко, В.А. Романюк. – К.: Наук. думка, 2012. – 444 с.

АНАЛІЗ МЕТОДІВ ПІДВИЩЕННЯ ЖИВУЧОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ЗВ'ЯЗКУ

Діджиталізація проникає в усі сфери людства та розкриває нові можливості взаємодії між людьми. Завдяки стрімкому розвитку технологій телекомунікаційні мережі (ТКМ) являють собою основний елемент рушійної сили прогресу. У зв'язку з цим до ТКМ постійно висуваються нові жорсткі вимоги та обмеження для того, щоб вони забезпечували потреби сьогодення, були адекватними завданням, які на них покладають, та гарантували якість обслуговування користувачів.

Враховуючи те, що під живучістю системи розуміють здатність системи виконувати передбачені їй функції в умовах зовнішніх та внутрішніх впливів, аналіз методів підвищення живучості є одним з важливих напрямків досліджень. Важливість ґрунтується на постійних змінах вимог до ТКМ у зв'язку з розвитком технологій та збільшенням кількості й урізноманітненням впливів, які діють на ТКМ в процесі її функціонування.

За результатами проведеного аналізу методів підвищення живучості ТКМ слід виділити наступні основні:

- метод підвищення живучості ТКМ шляхом реконфігурації мережі, оснований на оцінці відносних змін показників живучості – величин середньозваженого максимального потоку та середньозваженого найкоротшого шляху в мережі, за допомогою яких формується середньозважена комплексна оцінка відносних змін показників живучості;

- метод оптимального резервування вузлового обладнання для забезпечення необхідного рівня параметра “посередництво”. Рішення задачі оптимального резервування дає можливість визначати структуру резерву вузлів мережі, що забезпечує стійке функціонування мережі з метою підвищення живучості функціонування інфокомунікаційної мережі;

- використання кільцевих топологій з можливістю автоматичного перемикання каналів при аварійних ситуаціях на резервні шляхи;

- метод підвищення живучості ТКМ шляхом зменшення передумов зовнішніх впливів, зумовлених людським фактором, в основі якого є підвищення кваліфікаційного рівня підготовленості персоналу (особового складу), що здійснює експлуатацію та обслуговування ТКМ;

- використання оптимізованих математичних апаратів при врахуванні постпроектних впливів під час проектування ТКМ;

- метод децентралізованого принципу управління, завдяки якому зменшується вразливість мережі за рахунок дублювання та розподілу функцій управління та контролю в ТКМ.

В результаті аналізу даних методів постає актуальне питання щодо оптимізації методик оцінки живучості, методик підвищення живучості ТКМ з врахуванням принципів побудови та стану існуючих мереж зв'язку, а також з врахуванням тенденцій розвитку технологій в світі.

Особливої уваги потребує розгляд питання підвищення живучості транспортних мереж, побудованих з використання радіорелейних та тропосферних засобів зв'язку, враховуючи середовище розповсюдження сигналу та частотний діапазон обладнання. Зазначене питання актуалізується глобальним підвищенням мобільності користувачів мережі та можливістю оперативної побудови мережі зв'язку з використанням вищевказаних засобів зв'язку. За результатами досліджень очікується отримання результату щодо пошуку оптимального варіанту застосування методик та їх удосконалення з метою підвищення живучості ТКМ.

МЕТОД АВТОМАТИЗАЦІЇ ПРОЦЕСУ ВИБОРУ МАРШРУТУ ПОЛЬОТУ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТУ ПРИ ПРОВЕДЕННІ ПОВІТРЯНОЇ РОЗВІДКИ

Актуальність. В даний час накопичений значний досвід по створенню безпілотних літальних апаратів (БПЛА), в той же час питання їх ефективного застосування залишається важливою науковою проблемою. Однією з найбільш актуальних задач забезпечення польотів є задача планування маршруту БПЛА при проведенні повітряної розвідки. Використання безпілотних літальних апаратів під час ведення бойових дій вимагає розроблення додаткових механізмів захисту їх від впливу засобів радіоелектронної боротьби та підвищення безпеки польотів в зоні виконання бойових завдань. При цьому під безпекою польотів слід розуміти и можливість автоматичного уникнення можливих зіткнень, і можливість роботи з складних тактичних умовах, і уникнення вогневого контакту з засобами протиповітряної оборони противника та інші завдання.

Постановка задачі. На вибір маршруту впливають такі чинники: обмежений час польоту, тактико-технічні характеристики БПЛА, кількість цілей та їх ранг, безпека польоту, множинність маршрутів. Із задачею планування маршруту БПЛА пов'язана необхідність розробки нових підходів і моделей для розрахунків маршруту в реальному масштабі часу.

Метою доповіді є розробка методу автоматизації процесу вибору маршруту польоту безпілотного літального апарату при проведенні повітряної розвідки з врахуванням вказаних чинників в реальному масштабі часу.

Основні положення. Запропонована методика базується на використанні дискретної моделі польоту БПЛА і розроблена з використанням теорії графів.

Для розробки дискретної моделі польоту БПЛА представимо політ як послідовне відвідування певних областей простору. Розіб'ємо простір пошуку маршруту на елементи, враховуючи наступне:

- елемент повинен бути досяжний з одного або декількох сусідніх елементів, щоб забезпечити безперервність маршруту польоту;
- у процесі досягнення деяких сусідніх елементів може змінюватися курс і висота;
- можливість досягнення наступного елемента простору залежить від поточного курсу, і мінімального радіуса розвороту із припустимим перевантаженням;
- кількість дискретних напрямків польоту буде тісно пов'язане з розмірами елемента простору й мінімальним радіусом розвороту з припустимим перевантаженням;
- можливості досягнення сусідніх елементів повинні бути симетричні. Тому довжина елемента повинна бути дорівнює ширині;
- точність розв'язку буде зростати зі зменшенням елемента простору й збільшенням кількості дискретних напрямків польоту.

Висота елемента простору визначається за допомогою номограм для визначення шляху в наборі висоти.

Простір пошуку маршруту може містити зони, заборонені для польоту й небажані для польоту. Можливий підхід до формального опису простору пошуку маршруту:

- вважаємо, що простір усередині елемента має однакові властивості;
- вважаємо, властивістю простору мультиплікативний штраф за прокладку маршруту польоту БПЛА через елемент простору.

Завдання автоматизації процесу визначення маршруту БПЛА зводиться до завдання пошуку найкоротшого шляху між двома вершинами на графу, що дозволить застосувати клітинний автомат для пошуку раціонального маршруту.

Висновок. Запропонований метод можливо використовувати при розробці засобів автоматизації визначення маршруту в перспективних безпілотних авіаційних комплексах.

ОБГРУНТУВАННЯ СТВОРЕННЯ СИСТЕМИ МОНІТОРИНГУ ГНСС СИГНАЛІВ

Глобальні навігаційні супутникові системи (ГНСС) все більш міцно входять до складу основних стратегічних ресурсів світової інформаційної інфраструктури.

На даному етапі розвитку ГНСС підвищується актуальність завдання моніторингу (контролю) стану системи і наданих нею навігаційних послуг та інформаційної підтримки споживачів.

Розширюється використання технологій на базі ГНСС в різних сферах діяльності, включаючи всі види транспорту (повітряний, водний і наземний), геодезичні роботи, диспетчерські та аварійні служби, дослідження в галузі наук про Землю, сільське господарство, вирішення завдань оборонного характеру тощо.

Основні цілі системи моніторингу:

- контроль відповідності характеристик ГНСС їх заявленим значенням в нормативних документах;
- цілодобовий контроль працездатності навігаційних космічних апаратів (НКА) і достовірності переданих ними навігаційних даних, виявлення перерв у використанні НКА за цільовим призначенням за результатами обробки даних регіональної мережі станцій;
- контроль характеристик державної мережі Системи координатно-часового та навігаційного забезпечення України (СКНЗУ) та інших операторів навігаційних послуг;
- безперервна інформаційна підтримка через інтернет і виділені канали зв'язку споживачів навігаційних послуг достовірною і своєчасною інформацією про статус ГНСС;
- участь в міжнародних проектах щодо моніторингу ГНСС: International GNSS Service(IGS), EUREF Permanent GNSS Network та інших;
- використання мережі приймачів ГНСС для моніторингу стану іоносфери, тропосфери, геомоніторингу, метеорологічних параметрів, в проектах космічної погоди, контролю шкал часу за сигналами ГНСС.

Зростання вимог до навігаційного обслуговування і значне розширення сфер використання ГНСС привели до появи принципово нових вимог до якості навігаційних послуг.

В першу чергу, виросли вимоги до їх точності, надійності, доступності та достовірності.

В рамках штатних схем управління навігаційними системами ГЛОНАСС і GPS, які спочатку створювалися, в першу чергу, для вирішення оборонних завдань, вже неможливо в повному обсязі забезпечити виконання вимог всіх категорій користувачів.

При вирішенні цієї проблеми в навігаційних системах GPS, ГЛОНАСС, а також більш сучасних GALILEO і Beidou, багаторазово зростає роль так званих функціональних доповнень – постійно діючих систем, що виконують, зокрема, моніторинг якості функціонування ГНСС і передають користувачам додаткову інформацію, що дозволяє останнім підвищити точність і достовірність вирішення координатно-часових та навігаційних задач.

Головна мета таких систем – виявити відхилення від штатного функціонування ГНСС і своєчасно інформувати про це користувачів.

АНАЛІЗ МЕТОДОВ ЗМЕНШЕННЯ ПІК-ФАКТОРУ В СИСТЕМАХ БЕЗПРОВОДОВОГО ШИРОКОСМУГОВОГО ДОСТУПУ

Підвищення ефективності застосування систем безпроводового широкосмугового доступу, що функціонують в умовах мультиплікативних перешкод є актуальним завданням. Але підвищення завадостійкості систем передачі та обробки інформації, як одного з показників ефективності, вступає в протиріччя з завданням збільшення іншого показника ефективності, а саме спектральної ефективності. В більшості випадків підвищення ефективності зазначених систем відбувається за рахунок використання ортогонального частотного мультиплексування (*OFDM, Orthogonal Frequency Division Multiplexing*) та багатоантенної системи (*MIMO, Multiple Input Multiple Output*). Однак, одночасний негативний вплив багатопробеневого поширення сигналу та висока мобільність абонентів погіршують завадостійкість безпроводових систем. Тому в даний час ведуться активні дослідження щодо розробки перспективних систем обробки сигналів. Багаточастотні сигнали з неортогональним частотним ущільненням (*SEFDM, Spectrally Efficient Frequency Devision Multiplexing*), розглядаються в якості однієї з альтернатив *OFDM*-сигналів для використання в системах бездротового широкосмугового доступу. Одним із загальних недоліків для *OFDM*- і *SEFDM*-сигналів є пік-фактор, який призводить до обмеження сигналу, і, як наслідок, появи смугового і позасмугового випромінювання. Крім того, виникають нелінійні спотворення сигналу, який передається, що погіршує, а в деяких випадках, унеможливорює модуляцію сигналу на приймальній стороні.

У технічній літературі широко представлені різні методи зниження пік-фактору *OFDM*-сигналів. Однак, в існуючих роботах відсутній аналіз пік-фактору *SEFDM*-сигналів в залежності від коефіцієнта ущільнення та методів маніпуляції і кількості піднесущих, що використовуються в сучасних бездротових широкосмугових системах, а також не розглянуті особливості *SEFDM*-сигналів, які пов'язані з їх формуванням і прийомом. Важливо відзначити, що пік-фактор многочастотного сигналу є випадковою величиною, його значення змінюються в залежності від конкретних значень модуляційних символів піднесущих, які застосовуються в даному символі.

Проведений аналіз дозволив виділити наступні методи зниження пік-фактору *SEFDM*-сигналів: 1) методи, які вимагають передачі додаткової інформації про операції, що виконуються передавачем. До цих методів можна віднести методи частково переданої послідовності (*Partial Transmit Sequence, PTS*), вибіркового відображення (*Selective Mapping, SLM*), а також метод на основі ковзного вікна (*SLW, Sliding Window*). Зазначені методи показали зниження пік-фактору на 2-3 дБ для малого числа піднесущих (менше 200). Перераховані методи не ефективні для випадку великої кількості піднесущих (більше 200) і мають велику обчислювальну складність; 2) методи, що не потребують передачі сторонньої інформації (наприклад, метод резервування піднесущих (*Tone Reservation, TR*). В основі методу *TR* лежить розширення спектру шляхом додавання піднесущих, кількість яких залежить від значень комплексних амплітуд, що впливають на величину зниження пік-фактора. В загальному випадку додані піднесучі ігноруються на прийомі. Для систем, що використовують близько 1000 інформаційних піднесущих, при додаванні 32 піднесущих розширення спектра становить близько 3%, при середньому зниженні пік-фактору на 1,6 дБ.

Окрему увагу при зниженні пік-фактору багаточастотних сигналів необхідно приділяти методам формування таких сигналів. Оскільки для формування *OFDM*- і *SEFDM*-сигналів використовуються алгоритми швидкого зворотного перетворення Фур'є (ОБПФ), то для формування багаточастотних сигналів з пониженим значенням пік-фактору важливо зберегти такий підхід, забезпечивши ефективне повторне використання результатів ОБПФ при пошуку символу зі зниженим пік-фактором, або застосовуючи ОБПФ зі зниженою розмірністю.

ПРОБЛЕМАТИКА ДІАГНОСТУВАННЯ НОВІТНІХ СИСТЕМ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ

Функціонування системи зв'язку Збройних Сил України, виконання покладених на неї завдань здійснюється за допомогою новітніх зразків телекомунікаційного обладнання. Контроль функціонування (вирішення завдань технічного діагностування) новітніх систем телекомунікаційного обладнання в даний час зводиться до декількох основних алгоритмів перевірки (як правило перед початком роботи) і включає перевірку на справність основних плат та схем вцілому. При цьому не враховується стан елементної бази, який при проведенні періодичних технічних оглядів здійснюється неефективно та поверхнево. В обмеженій кількості існують системи глибокого контролю. Однак ці системи дорогі та застосовуються виключно в критичній інфраструктурі. Тому актуальність створення системи діагностування яка б забезпечувала надання достовірної інформації про фактичний стан елементної бази новітнього телекомунікаційного обладнання є досить високою.

Якість та ефективність такої діагностики та контролю параметрів ускладнюється надзвичайно великою кількістю технологічних процесів які відбуваються в телекомунікаційному обладнанні, їх апаратних та програмних складових. Це різноманіття виражене у використанні компонентів високого ступеня інтеграції (мільйони інтегрованих елементів на кристалі компонентів системної логіки), мікронною технологією розведення провідників на кристалах інтегральних мікросхем (0,13-0,18 мкм), багатошаровими друкованими платами з кроком рознесення виводів друкованих провідників менше 0,5 мм відсутністю внутрішніх контрольних точок і т.д.

Проведений аналіз основних несправностей сучасного телекомунікаційного обладнання показав, що основною причиною його відмов є несправність блоків живлення (90% від загальної кількості несправної апаратури). Враховуючи велику кількість наявних зараз зразків та модифікацій телекомунікаційного обладнання практичний інтерес викликає створення уніфікованої автоматизованої системи діагностування замість багатьох різновидів адаптованих під різні зразки блоків та плат. Таким чином в структурі автоматизованої системи діагностування необхідно передбачити підсистему контролю блоків живлення з імпульсним стабілізатором безтрансформаторного типу які є найпоширенішими в новітньому телекомунікаційному обладнанні. При цьому доцільно передбачити можливість контролю обраного типу устаткування як в складі телекомунікаційного обладнання так і окремо від нього.

Оскільки процес контролю та діагностування на різних етапах життя мікропроцесорної елементної бази характеризується різними діагностичними, технологічно-відмінними операціями, варто зауважити що однозначного підходу до вирішення цієї проблеми немає.

Наявні на сьогодні методи такі як діагностування за допомогою одношарової нейронної мережі Хопфілда, що відображають комбіноване поетапне діагностування телекомунікаційного обладнання в процесі всього життєвого циклу є трудомісткими та мають недоліки серед яких неоднозначність вхідних і вихідних значень.

Розроблення більш досконалих методів діагностування на платформі нейронних систем (як систем зі зворотнім зв'язком) з використанням мови програмування Пайтон дасть можливість з високою точністю класифікувати числа вхідних і вихідних значень контрольованих параметрів мікроелементної бази. Забезпечить можливість значно підвищити якість контролю параметрів та покращити ефективність діагностування новітнього телекомунікаційного обладнання вцілому.

АНАЛІЗ РЕАЛІЗАЦІЇ ФІШИНГОВИХ АТАК НА МЕРЕЖУ ІСД-ІНТЕРНЕТ

Актуальність. В умовах інформаційної війни важливого значення набуває інформація, яка є стратегічним ресурсом. Протягом останніх років все ширше використання перспективних інформаційних технологій зумовило не лише численні переваги, а й цілу низку проблем. Істотно підвищився рівень інформаційного негативного впливу на процеси збереження та розповсюдження інформації, зросла чисельність нових форм кібератак.

Аналіз останніх публікацій. Згідно статистичних даних представлених у звіті *Anti-Phishing Working Group* загальна кількість фішингових атак, виявлених у 2 кварталі 2020 року, склала 146 994, що на 20% менше порівняно з 2 кварталом 2019 року (182 465), та на 6% більше ніж у 2 кварталі 2018 року (138 288).

Виклад основного матеріалу дослідження. Інформаційна система з доступом до мережі Інтернет (далі – ІСД-Інтернет) призначена для забезпечення доступу та використання інформаційних ресурсів мережі Інтернет службовими особами МОУ та ЗС України. Головною метою системи є обмін відкритою інформацією (електронна пошта, офіційні сторінки в соціальних мережах) у службових цілях. Також система забезпечує функціонування інших інформаційних систем МОУ та ЗС України.

Структура мережі складається з головного вузла, регіональних вузлів, територіальних вузлів, АРМ ІСД-Інтернет та комплексів контролю безпеки інформації.

Забезпечення безпеки інформації в ІСД-Інтернет здійснюється шляхом впровадження комплексних систем захисту інформації на АРМ та виконання заходів з безпеки інформації на головному, регіональних та територіальних вузлах мережі, а також заходів з контролю безпеки інформації. Для виключення несанкціонованого доступу до мережі та контролю використання комп'ютерних програм користувачами застосовується доменна структура з використанням групових політик безпеки на базі ОС Linux та/або MS Windows Server.

Фішинг — це кібератака з використанням соціальної інженерії, що дозволяє отримувати інформацію, яку можна використовувати для доступу до пристроїв або мереж. Цей тип атаки застосовує певні технології, щоб замаскувати комунікації або веб-сторінки під надійне джерело.

Основною метою фішингу є отримання доступу до конфіденційних даних користувачів (логінів і паролів). Це досягається шляхом проведення масових розсилок електронних листів, в яких міститься пряме посилання на сайт, ззовні схожий на справжній, або на сайт з перенаправленням. У випадку переходу на «фейкову» сторінку, противник намагається різними психологічними прийомами спонукати користувача ввести свої персональні дані.

Цільовий фішинг спрямований на конкретну особу або компанію з використанням спеціально зібраної інформації про ціль з відкритих джерел (соціальні мережі, періодичні публікації, офіційний сайт організації), щоб зробити своє послання-прийом переконливішим.

До технологій мережної безпеки відносяться захист електронної пошти та веб-ресурсів, захист від шкідливого ПЗ, відстеження поведінки користувачів і контроль доступу. Сучасні веб-переглядачі включають служби безпечного перегляду, які увімкнені вже за замовчуванням. Найефективнішим методом захисту є багаторівневий підхід, який призначений для зменшення кількості атак і зниження рівня впливу в разі їх здійснення.

Одним із способів захисту організації від фішингових атак є навчання користувачів. Розпізнавання фішингових листів і вживання належних дій при їх отриманні має охоплювати всіх співробітників.

Висновок. Система ІСД-Інтернет має свою систему захисту інформації, але постійне збільшення фішингових атак та застосування нових методів для їх успішної реалізації вимагають подальших дослідження в цьому напрямку.

ОЦІНКА ШВИДКОДІЇ ПРОГРАМНИХ ФУНКЦІЙ СКАЛЯРНОГО МНОЖЕННЯ З ВИКОРИСТАННЯМ MIRACL CRYPTOGRAPHIC SDK

Актуальність. Все більшої популярності набувають криптосистеми побудовані на еліптичних кривих через те, що на основі їх застосування вдалося забезпечити ті ж показники стійкості, якими володіють числові і поліноміальні криптосистеми, але відповідні показники перших вдалося отримати при істотно меншому розмірі ключа.

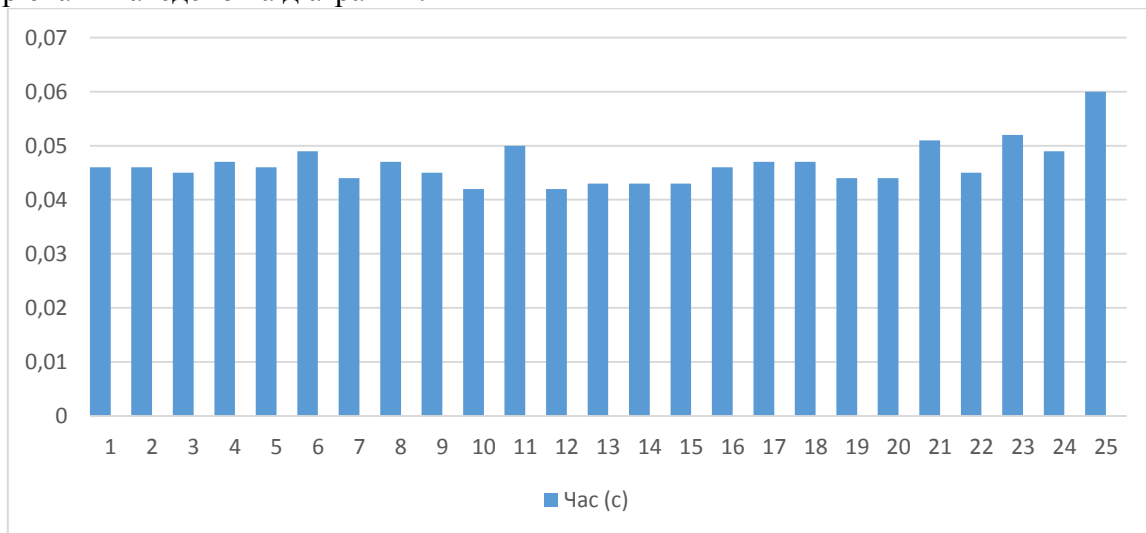
Мета. Метою роботи є оцінка швидкодії програмних функцій скалярного множення з використанням MIRACL Cryptographic SDK.

Основна частина. Операція скалярного множення являє собою множення цілого числа n на точку P еліптичної кривої. Обчислення nP вимагає n додавань точки P , що є найбільш ресурсо- та часовитратною операцією, тому актуальними є дослідження способів та методів даного обчислення.

Скалярний добуток точок кривих Едвардса обчислюється мінімальним числом операцій, тому вони викликають інтерес при проектуванні криптографічних протоколів і стандартів асиметричного шифрування. Порівняння швидкості виконання операції скалярного множення на кривих Едвардса та Вейерштрасса показало, що криві Едвардса дають приріст швидкості скалярного множення приблизно в 1.5 рази та є лідером в швидкості обчислення.

Для програмної реалізації операцій над точками еліптичних кривих було використано MIRACL Crypto SDK, що є золотим стандартом SDK з відкритим кодом для криптографії еліптичної кривої (ECC). Бібліотека MIRACL складається з понад 100 процедур, які охоплюють усі аспекти високоточної арифметики.

Дослідження швидкодії програмної функції скалярного множення було проведено для точок еліптичних кривих з характеристиками поля 256, 384 та 512 біт. Результати вимірювань наведено на діаграмі 1.



Діаграма 1. Час виконання програмної функції скалярного множення для точок ЕК Едвардса з бітовою величиною характеристики поля 512 біт

Середній час виконання скалярного множення для точок ЕК Едвардса з бітовою величиною характеристики поля 512 біт висновок, що $t_{\text{сер}} \approx 0,047$ (с).

Висновок. Отримано нові результати оцінки швидкодії операцій скалярного множення точок кривих Едвардса, а також нові параметри часткового випадку еліптичних кривих, що надають можливість отримати максимальну швидкодію операцій над точками еліптичної кривої, що дозволені міжнародними стандартами для криптографічного застосування.

АКТУАЛЬНІ ПИТАННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Кібербезпека є однією з найбільш системно важливих проблем, з якими стикається сьогодні світ. Протягом останніх десяти років кібербезпека перетворилася у головну стратегічну тему глобального значення.

Зростання важливості кібербезпеки як проблеми неодноразово зазначалось у звітах Світового економічного форуму щодо глобального ризику, і зараз потенційні загрози від кібератак, фроду, кіберстійкості критичних інформаційних інфраструктур постійно класифікується як один з найбільших глобальних ризиків, з яким стикається сьогодні світова економіка.

Активна політика керівництва країни щодо повного й всеохоплюючого переходу на цифрові технології, впровадження багатьох необхідних для громадськості та країни проєктів, що стосуються цифрової економіки, розвитку фінансового сектора, електронного урядування, цифрових інфраструктур, а також заходи щодо боротьби з пандемією COVID-19 призвели до необхідності прискореної цифрової трансформації у багатьох сферах, що відповідно збільшує залежність національної економіки від цифрової інфраструктури.

В якості світового тренду також відзначається збільшення фінансових втрат від кібератак, порушення цілісності і безперервності функціонування в тому числі фінансового ринку.

Специфічність методів, способів і засобів вчинення кібератак та вимагає від регуляторів гнучкості, оперативності, використання інноваційних, сучасних цифрових технологій і методів кіберзахисту.

Все це посилює виклики кібербезпеки, які існували раніше, але також продемонструвало всім зацікавленим сторонам необхідність та стимул для вирішення стратегічних проблем пов'язаних із забезпеченням високого рівня кіберстійкості фінансової системи та країни в цілому.

Враховуючи сучасні тренди в сфері стратегічних цілей та завдань в сфері кібербезпеки провідних країн світу, Стратегію розвитку фінансового сектора до 2025 року та прийняту нову Стратегію національної безпеки, та роботу яка наразі проводиться щодо розробки нової Стратегії кібербезпеки України, пропонуємо таке.

Політика Національного банку з питань кібербезпеки повинна бути направлена на застосування ефективних стимулюючих, регуляторних, просвітницьких та контролюючих заходів щодо зменшення потенціалу наслідків від кіберінцидентів та кібератак стосовно надання банківських та фінансових послуг, що мають вирішальне значення як для суспільства, так і для національної та міжнародної фінансової системи, яка може підірвати безпеку та довіру безпеці та стабільності фінансової системи та загрожувати економічному зростанню країни.

У новій Стратегії кібербезпеки України, в частині організації та забезпечення кібербезпеки у фінансовому секторі, пропонуємо передбачити реалізацію таких заходів, програм та ініціатив:

закріплення на законодавчому рівні повноважень Національного банку України щодо державного регулювання, через встановлення відповідних вимог, правил та порядку, здійснювати нагляд і контролю, а також застосовувати заходи впливу з питань кіберзахисту та інформаційної безпеки в фінансовій сфері;

імплементація в національне законодавство кращих передових практик та настанов, щодо регулювання та нагляду з питань кібербезпеки у фінансовій сфері таких провідних організацій, як: European Central Bank, European Banking Authority, Bank of International Settlements, Financial Stability Board, International Monetary Fund, International Association of Insurance Supervisors, International Organization of Securities Commissions, Committee on Payments and Market Infrastructure та інш.;

запровадження сучасних технологій – RegTech та SupTech до регуляторних, наглядових/контролюючих заходів з питань кіберзахисту в фінансовій сфері;

подальший розвиток та вдосконалення створеної інфраструктури центрів кіберзахисту, команд реагування на комп'ютерні надзвичайні події, удосконалення механізмів обміну інформацією про актуальні і потенційні кіберзагрози, автоматизація її обробки та застосування;

розвиток транскордонної співпраці з питань кібербезпеки, в частині обміну інформацією про кібератаки з метою запобігання, розслідування та попередження транскордонних кіберзагроз, кіберзлочинів;

створення та розвиток інститутів незалежного аудиту інформаційної безпеки, тестування та оцінки кіберстійкості суб'єктів забезпечення кібербезпеки з урахуванням кращої практики європейських держав;

запровадження практики проведення кібер-стрес-тестувань фінансових установ і періодичних кібернавчань щодо реагування на кіберзагрози та кіберкризи в фінансовій сфері;

відродження інститутів акредитації органів сертифікації та оцінки відповідності міжнародним стандартам, які останнім часом широко використовуються в Україні для вирішення питань забезпечення інформаційної та кібербезпеки;

створення державної системи сертифікації, експертизи засобів електронної ідентифікації, а також підтвердження еквівалентності засобів електронної ідентифікації прирівняних до ідентифікації особи, здійснених в її присутності;

розширення кола питань державно-приватного партнерства та державно-приватної взаємодії у сфері забезпечення безпеки кіберпростору та захисту інформаційних ресурсів;

створення умов та вжиття заходів для зниження рівня кібершахрайства в фінансовій сфері;

сприяння у проведенні та організації конференцій, семінарів, круглих столів, тренінгів, навчань з питань кібербезпеки у фінансовій сфері.

створення умов для розвитку культури інформаційної безпеки в фінансовій сфері та реалізація на постійній основі державних програм підвищення фінансової кіберобізнаності населення.

Реалізація запропонованих заходів, на наш погляд, сприятиме подальшому розвитку та вдосконаленню регуляторної та наглядової політики держави в сфері кібербезпеки, підвищить ефективність заходів кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури.

МОДЕЛЬ ЗАСТОСУВАННЯ СЕРВЕРНИХ СИСТЕМ В КОНЦЕПЦІЇ ІНТЕРНЕТУ ВІЙСЬКОВИХ РЕЧЕЙ (ІОВТ)

В умовах сучасних швидкоплинних та високо маневрених бойових дій отримання переваги над супротивником вимагає організації взаємодії між угрупованнями військ шляхом налагодження безперервного та надійного управління територіально-рознесеними підрозділами, які розміщені на значних географічних територіях. У зв'язку з цим у комплексі заходів із забезпечення національної безпеки розвинених країн світу пріоритетним стає питання, пов'язане із використанням досягнень в області новітніх інформаційних і телекомунікаційних технологій для розвитку і удосконалення серверних систем в концепції інтернету військових речей як одного із головних елементів державної і воєнної інфраструктури, який визначає ефективність застосування військ (сил) та озброєння.

Основними особливостями сучасних бойових дій, а також процесів управління військами, бойовими системами і озброєнням є встановлення, що концепція Інтернету речей має три взаємопов'язані базові проблеми – це забезпечення інформаційної безпеки (*Internet of Things Security*), масштабування зростаючого обсягу технічних пристроїв і даних (*Internet of Things Scalability*), а також урахування вимог до зниження енергоспоживання (*Internet of Things Technical Solutions and Low-Power Consumption*).

На основі вищезазначеної проблематики було розглянуто побудову платформи для розгортання системи моніторингу, контролю доступу та охорони військових (спеціальних об'єктів) за допомогою новітніх підходів до розробки розподілених систем прийому, зберігання та обробки великих обсягів даних. Для побудови платформи використано сучасне програмне та апаратне забезпечення, досліджено розгортання платформи у хмарному хостингу. Запропоновано архітектуру програмного забезпечення, яка забезпечує її високу масштабованість і ефективність, а також дозволяє реалізувати рішення для моніторингу мережі пристроїв і роботи з адміністративними даними, які є більш функціональними за існуючі. Реалізація вищезазначених вимог можлива лише за використання систем обробки первинного інформаційного трафіку та аналітики. Зазначена підсистема (охорона військових частин спеціальних об'єктів ЗСУ) включає в себе автоматизовані робочі місця адміністраторів баз даних і відповідних фахівців, які приймають, обробляють та аналізують первинний інформаційний трафік. Автоматизовані робочі місця адміністраторів розподіляють доступ відповідно до фіксованих повноважень, узгоджують надходження і видачу даних, а також забезпечують захист даних і їх вчасне відновлення у випадку збоїв і аварій різноманітного характеру. Автоматизовані робочі місця фахівців, які є забезпеченими необхідними технічними програмними засобами і сучасним високошвидкісним зв'язком, здійснюють попередній аналіз первинного інформаційного трафіку, його уніфікацію, занесення до відповідних баз даних, моделюють кризові ситуації і відпрацьовують плани виходу з них.

Отже, у даній роботі було зроблено моделювання предметної області операційних систем для розгортання серверів було зроблено висновок, щодо використання хмарної системи для підтримки (*IoBT*). У даній дипломній роботі також було проведено аналіз (*IoT*), після якого було зроблено висновок для кращого використання *IoT* в армії. Після цього було виконано завдання щодо моделювання технологій та засобів створення програмних модулів та їх інтерфейсів. дуже важливо, щоб як хмара, так і *IoBT* формували хмарні додатки *IoBT*, щоб максимально використати їх комбінацію. На додаток до цього, ще кілька показників, чому хмара важлива з точки зору успіху *IoBT*. Хмара як технологія дає можливість *IoBT* вийти за межі звичайної техніки, наприклад, термометр, гідрометрів тощо. Зі збільшенням мініатюризації та переходу з 4G на більш високі швидкості Інтернету, хмарні технології дозволять розробникам швидко розвантажувати великі за обсягом обчислювальні процеси.

Радченко М.М. (НЦЗІ ВІТІ)
Драглюк О.В. (НЦЗІ ВІТІ)
Коротков М.М. (НЦЗІ ВІТІ)
Бригадир С.П.(НЦЗІ ВІТІ)
к. економ. н. Маланчук М. Ф. (ННЦОМ НАОУ ім.Черняхівського)

ОСОБЛИВОСТІ СИСТЕМ ОБОРОННОГО ПЛАНУВАННЯ В США ТА В УКРАЇНІ

Актуальність. У перші роки існування незалежної України оборонне планування здійснювалося за інерцією на основі застарілих радянських поглядів, які не відповідали новим політичним та економічним реаліям. Основним орієнтиром було стрімке згортання воєнного потенціалу держави з метою скорочення необхідних для його підтримання витрат. Він мав місце до 2014 року і призвів до скорочення бойових спроможностей Збройних Сил України, занепаду оборонно-промислового комплексу держави. Найбільш доцільним шляхом проведення реформування та реорганізації системи оборонного планування, оборонного замовлення та, відповідно, оборонно-промислового комплексу України є вивчення та впровадження передового зарубіжного досвіду в організації та методології наукового супроводження цього процесу

Досвід НАТО показує, що запроваджені в країнах Альянсу підходи до планування на основі спроможностей дали змогу перейти до концепції розвитку сил оборони країн-партнерів за принципом “ефективність на противагу кількості” та здійснити функціональну інтеграцію процесів оборонного і бюджетного планування. Кінцевою метою такого планування є формування на підставі прогнозованих економічних умов комплексних спроможностей сил оборони, достатніх для гарантованого виконання визначених завдань.

Оборонна реформа України визначає одним з головних напрямів зосередження зусиль – це вдосконалення оборонного планування.

Метою доповіді є розгляд особливостей оборонного планування США та України як шлях визначення найбільш прийняттого підходу щодо планування на сучасному етапі реформування й розвитку в секторі безпеки і оборони України.

Основні положення.

У відповідності з діючими в США нормативно-правовими документами міністерства оборони (далі – МО) від ідеї до поставки у війська об’єкту військової техніки повинні здійснитися наступні процеси:

1. Визначення вимог до зразка військової техніки в Системі інтеграції та розвитку спільних спроможностей (The Joint Capabilities Integration and Development System – JCIDS);
2. Виділення фінансових ресурсів та асигнувань в Системі планування, програмування, бюджетування та виконання (PPBE);
3. Розробка, випробування та закупівля в Системі оборонного замовлення (DAS).

Процеси JCIDS, PPBE та DAS є тісно пов’язаними та здійснюються одночасно з урахуванням повної кооперації та координації зусиль. Затвердженні вимоги до об’єкту замовлення військової техніки JCIDS забезпечують основу для визначення продукції, що буде закуповуватись, PPBE визначає пріоритети МО, здійснює розподіл ресурсів та спрямовує кошти, необхідні для виконання запланованих програм. Протягом всього життєвого циклу продукції є можливим здійснення коригувань з метою синхронізації процесів наведених вище.

В МО США процес визначення вимог (кількісно-якісних показників) до зразка озброєння та військової техніки (далі – ОВТ) здійснюється в Системі інтеграції та розвитку спільних спроможностей а в Україні – Системою наукових досліджень що наведено в порівняльній Таблиці 1. JCIDS допомагає виявити проблемні питання в можливостях зразку ОВТ та на основі їх аналізу сформулювати пропозиції щодо вирішення їх організаційним шляхом або шляхом придбання (розробки) ОВТ. Результати JCIDS формують граничні умови для етапу аналізу альтернатив, які проводяться у подальшому в Системі оборонного

замовлення. Якщо результатом є рекомендація щодо створення зразка (комплексу, системи) ОВТ, то розробляються і затверджуються вимоги за призначенням.

Таблиця 1

Порівняльна таблиця відповідності елементів визначення вимог та створення зразка ОВТ

США			Україна		
Система інтеграції та розвитку спільних спроможностей (JCIDS)			Система наукових досліджень щодо визначення кількісно-якісних показників ОВТ		
Рада спільних вимог (Joint Requirements Oversight Council – JROC) здійснює:	Оцінка	Capabilities Base Assessment – CBA (Наявні спроможності)	Замовник ОВТ здійснює:	Оцінка	Кількісно-якісний склад системи озброєння
	Затвердження	Initial Capabilities Document – ICD (Початковий огляд спроможностей)		Розробка	Оперативно-тактичні вимоги до ОВТ
	Затвердження	Capability Development Document – CDD (Вимоги до розроблення спроможностей)		Розробка	Загальні-тактичні вимоги до ОВТ
		Key Performance Parameters – KPP (Основні функціональні параметри, які визначаються по CDD). Оцінюються вартісні ризики при забезпеченні цих параметрів; визначаються часові періоди та ступінь розвитку технологій; оцінюються вартість системи у порівнянні з функціональною спроможністю, що забезпечується цією системою		Розробка	Тактико-технічне завдання на проведення дослідно-конструкторської роботи (тактико-технічні та техніко-економічні вимоги до ОВТ; вимоги до матеріалів, комплектуючих виробів та за видами забезпечення; вимоги до навчально-тренувальних засобів та інш.)
	Затвердження	Capability Production Document – CPD (Вимоги до виробництва спроможностей). Їх мета - контроль відповідності ОВТ, що постачається у війська, вимогам, які визначені ICD, у тому числі щодо вартісних показників. У CPD зосереджена інформація, що використовується при виробництві та експлуатації ОВТ, а також для перевірки його працездатності		Розробка	Програма та методики випробувань
				Укладання	Контракт та перегляд (доповнення) ТТЗ в ході проведення ДКР

Наступну ступінь процесу поставки зразку ОВТ характеризує Система планування, програмування, бюджетування та виконання (PPBE), яка щорічно створюється у МО і надається до Конгресу США оборонної частини Бюджету Президента та визначає пріоритети і цілі програм закупівель МО, спрямована на управління фінансами (розподіл ресурсів) поточних та майбутніх програм (Таблиця 2).

В Україні системі PPBE умовно відповідає Система оборонного планування розвитку ОВТ (Таблиця 2). З прийняттям Закону України “Про національну безпеку” вона, за сутністю стратегічно-концептуальних документів та структурною побудовою програмних документів середньострокового і короткострокового планування, практично повністю почала відповідати Системі планування, програмування, бюджетування та виконання в США. Відмінністю є лише різниця в термінах бюджетних пропозицій міністерства оборони США, які надаються на два роки а Державне оборонне замовлення в Україні - складається на термін до трьох років. Розробка програмних пропозицій до Меморандумів про цілі програм (Program Objective Memorandum – POM) супроводжується їх балансування таким чином, щоб відповідати напрямам та пріоритетам, визначеним Керівництвом з системи оборонного замовлення з урахуванням фінансових обмежень. POM усіх структурних підрозділів МО узагальнюються та складається Середньострокова оборонна програма (Future Year Defense Program – FYDP), яка після затвердження міністром оборони є фінансовим планом МО, охоплює 5-річний період (бюджетний рік та 4-и наступних роки) та щорічно оновлюється під

час складання POM. FYDP об'єднує відомості всіх структурних підрозділів МО за програмними елементами, які включають сукупність функціональних або організаційних заходів та пов'язаними з ними фінансовими ресурсами залежно від цілей.

Таблиця 2

Відповідність елементів Системи планування, програмування, бюджетування та виконання в США та Системи оборонного планування розвитку ОВТ в Україні

США			Україна		
Система планування, програмування, бюджетування та виконання (The Planning, Programming, Budgeting, and Execution System)			Система оборонного планування розвитку ОВТ		
Етапи:	Планування	Визначення та розгляд альтернативних стратегій, аналіз тенденцій та умов, що змінюються, оцінка можливих загроз, наявних технологій та економічних оцінок в поєднанні з прогнозуванням довгострокових наслідків та ймовірних змін. На цьому етапі розглядаються та визначаються потреби МО на наступні 5, 10, 20 та більше років.	Етапи:	Планування	Створення стратегічно-концептуальних документів та програмних документів середньострокового і короткострокового планування
	Програмування	Розроблення програмних пропозицій до Меморандумів про цілі програм (Program Objective Memorandum – POM). Складається Середньострокова оборонна програма (Future Year Defense Program – FYDP)		Програмування	Розроблення програмних пропозицій до Концепції Державної цільової оборонної програми розвитку
	Фінансування	Процес формування та обґрунтування бюджетних показників перших двох років FYDP для гарантування ефективного використання ресурсів.		Фінансування	Державна цільова оборонна програма розвитку ОВТ (передбачає науково-технічне супроводження ДЦОПР ОВТ)
	Виконання	Безпосереднє виконання процесу РРВЕ. Надає зворотній зв'язок вищому керівництву стосовно ефективності попереднього та поточного розподілу ресурсів. Під час виконання програми оцінюються відповідність встановлених показників її ефективності. У разі, якщо цілі програми не виконуються, надаються рекомендації щодо використання ресурсів або зміни структури програми з метою досягнення цілей програм.		Виконання	Державне оборонне замовлення (передбачає науково-технічне супроводження ДКР)

В Україні за процес розробки та закупівлі озброєння відповідає Система Державного оборонного замовлення (Таблиця 3). Його основою є Система розробки та постановки на виробництво, яка визначає порядок виконання дослідно-конструкторських робіт та на даний час розробляється в Україні на основі стандартів серії В 15. Крім того, процес Державного оборонного замовлення регламентується відповідними Законами та постановами Кабінету Міністрів України. Етап Розроблення технологій та підготовки виробництва в Україні за своєю сутністю відповідає етапу Розвиток технологій та зменшення ризиків в США. В його основі покладена Єдина система технологічної підготовки виробництва, що регламентується ГОСТами серії 14. Система оборонного замовлення DAS являє собою управлінський процес, за допомогою якого МО США купує та розробляє ОВТ. Процеси, що описані в документах DAS, в деякій мірі схожі з процесами існуючої в Україні системи розробки та постановки на виробництво (СРПВ). Порядок управління всіма програмами закупівель встановлює Інструкція МО США “Функціонування системи оборонних закупівель”. В залежності від загального обсягу фінансування та важливості вони поділяються на три категорії: I категорія (АСАТ I) – якщо обсяг фінансування на НДДКР більше 480 млн дол., або в цілому на закупівлю – більше 2,79 млрд дол. (в цінах 2014 р.); II категорія (АСАТ II) – якщо на НДДКР – більше 185 млн дол., або в цілому на закупівлю – більше 835 млн дол.; III категорія (АСАТ III) – менш, ніж визначено для II категорії. Розроблення та підготовка виробництва

(Engineering and Manufacturing Development – EMD) є офіційним початком програми закупівлі, який спрямований на розроблення, виготовлення та випробування ОВТ для підтвердження їх відповідності оперативним вимогам.

Таблиця 3

Системи оборонних замовлень США та України

США			Україна	
Система оборонного замовлення (DAS)			Сист. Держ. оборонного замовлення (вкл. в себе Систему розробки та постановки до виробництва (СРПВ))	
Етапи:	Розвитку технологій та зменшення ризиків	Перевірка задоволення вимогам ACAT I, ACAT II, ACAT III	Етапи:	Формування ДОЗ (згідно ЗУ “Про ДОЗ”, ПКМУ “Деякі питання ДОЗ”)
		MSA (Materiel Solutions Analysis) – аналіз матеріальних рішень. Рішення про розробку приймається на основі затвердженого Початкового огляду спроможностей. Стратегія закуп. (виготовлення). Ріш. за етапом.		Проведення тендеру (згідно ЗУ “Про проведення тендеру”) Аванпроект (згідно ГОСТ В 15.103)
	Розробки та підготовки виробництва	Розвитку технологій та зменшення ризиків (Technology Maturation and Risk Reduction – TMRR)		Створ. зразків ОВТ в ініц. порядку (згід. ДСТУ В 15.203). Вик-ня ДКР.
		Попередній технічний огляд (Preliminary Design Review – PDR) майбутнього виробу, ще до вибору виконавця.		Розробка технологій та підготовка виробництва (Єд. сист. технол-ї підгот. виробництва. ГОСТ В 14.)
		Розробка та підготовка виробництва (Engineering and Manufacturing Development – EMD).		Державні випробування (прийняття на озброєння) (ДСТУ В 15.210)
		Ріш. про схвалення CDD; Ріш. про Запит пропозицій щодо розробки (Request for Proposals – RFP) від підприємств промисловості; Ріш. про уклад. контракту на розр-ку (Decision to award the contract)		
	Виробництво та постачання продукції до військ	Рішення про виробництво установочної партії (Low-Rate Initial Production – LRIP), або Рішення про обмежене постачання (Limited Deployment Decision)		Виробництво зразків ОВТ (згідно ГОСТ В 15.301)
		Рішення про серійне виробництво (Full Rate Production Decision – FRPD) або Рішення про постачання до військ (Full Deployment Decision):		Постачання ОВТ до військ ()
	Експлуатація та утилізація ОВТ	Етап Операцій та підтримки (Operations and Support – O&S). Робота здійснюється згідно Плану підтримки житлового циклу зразку ОВТ (Life Cycle Sustainment Plan) – LCSP		Експлуатація ОВТ (згідно Плану утримання)

Висновки. Таким чином з наведених особливостей систем оборонного планування США та України випливає що національна Система розроблення та постачання на виробництво ОВТ продовжує реформуватися. Втілюються нові організаційно-правові підходи, проводиться робота щодо зміни методології планування та переведення підходів планування розвитку ЗС “на основі спроможностей”. Здійснюється процес вирішення багатьох проблемних питань обґрунтування остаточного вигляду такої системи в Україні виходячи із існуючих відмінностей між країнами як у структурах і розмірах ЗС, економічних відносинах, потужностей підприємств оборонної промисловості, так і у обсягах фінансування потреб оборони. Разом з тим, доцільно зазначити, що реорганізацію системи оборонного планування в Україні шляхом впровадження процедур та принципів системи оборонного планування США необхідно здійснювати з урахуванням особливостей оборонно-промислового комплексу України. Реорганізація існуючої адміністративної системи управління оборонним плануванням потребує створення відповідного нормативно-правового забезпечення та розробки науково-методичного забезпечення на кожному етапі названого процесу.

ІНТЕРАКТИВНА ПЛАТФОРМА ТЕСТУВАННЯ ВІЙСЬКОВОСЛУЖБОВЦІВ НА ОСНОВІ СЕРВЕРУ ДОДАТКІВ ТОМСАТ

Актуальність теми. Навчання військовослужбовців, зокрема курсантів ВВНЗ, є важливою частиною підтримки боєздатності військ у мирний час та складовою забезпечення ефективності застосування військ у воєнний час.

Виконання посадових обов'язків викладачами вищих навчальних закладах, інструкторами, командирами підрозділів, які задіяні до проведення занять з особовим складом та здійснюють відповідне оцінювання, на даний час занадто ускладнене рутинними процесами (перевірка тестів вручну, генерація ключів-відповідей, друк бланків тощо). Таким чином, існує протиріччя між потребою у раціональному розподілі службового часу та необхідністю виконання значної кількості рутинних операцій при оцінюванні тих, хто навчається. Одним із шляхів вирішення вказаного протиріччя є застосування автоматизованих засобів навчання. Часові затрати на розробку таких засобів можуть бути значними, але в майбутньому це позитивно вплине на ефективність роботи науково-педагогічного складу та якість освіти в цілому. Враховуючи наведене вище, виникає необхідність у розробці платформи тестування як засобу навчання, що дозволить частково автоматизувати визначені рутинні процеси діяльності науково-педагогічних працівників.

Мета роботи: підвищити ефективність роботи науково-педагогічного складу військових підрозділів за рахунок впровадження інтерактивної платформи тестування.

Для досягнення вказаної мети у роботі сформульовано наступні **часткові завдання**:

- 1) провести аналіз нормативних та керівних документів, які регламентують організацію навчального процесу у вищих навчальних закладах;
- 2) дослідити функціональність існуючих інтерактивних платформ тестування з відкритим вихідним кодом та можливість їх застосування у вищих навчальних закладах;
- 3) розробити структурну схему та алгоритм функціонування платформи тестування;
- 4) за результатами проєктування реалізувати відповідне програмне рішення.

Виклад основного матеріалу.

Програмний додаток розроблено мовою Java з використанням фреймворку Spring. Додатково у роботі застосовано наступні технології: Spring Boot, Spring MVC, Spring Security, Hibernate, СКБД MySQL, HTML, CSS, Bootstrap, Apache Freemarker.

Варіанти взаємодії того, хто навчається з платформою тестування включають авторизацію, проходження тестування, перегляд результатів та зміну особистих даних в персональному кабінеті. Функціональність в режимі адміністратора передбачає авторизацію, створення тесту, завантаження готового тесту, зміну прав користувачів, отримання результатів статистичної обробки успішності та генерацію звітних матеріалів.

Висновки. Під час вирішення сформульованого у роботі завдання проаналізовано керівні документи, які регламентують організацію освітнього процесу у вищих навчальних закладах, обґрунтовано доцільність розробки платформи тестування, яка б відповідала встановленим до цього класу програмного забезпечення вимогам. Спроєктовано діаграми варіантів використання та діаграму класів тестувальної платформи, які відображають функціональні можливості взаємодії курсантів та НПП з програмним рішенням. Розроблено архітектуру програмного додатку, обрано засоби та технології реалізації.

Застосування запропонованого у роботі програмного додатку дозволить автоматизовано проводити тестування з подальшим оцінюванням результатів, внаслідок чого ефективність роботи НПП підвищиться. Також додатково з'являється можливість здійснювати контроль успішності тих, хто навчається шляхом моніторингу статистики результатів тестування та аналізу тенденцій успішності за визначений період часу.

МОДУЛЬ РЕЄСТРАЦІЇ, АВТЕНТИФІКАЦІЇ ТА АВТОРИЗАЦІЇ ЗА ДОПОМОГОЮ СТАНДАРТУ OAuth2 КОРИСТУВАЧА КОМПЛЕКСУ СПЕЦІАЛІЗОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ „ПЛАТФОРМА НИЗОВОГО МОНІТОРИНГУ ОБ’ЄКТІВ БУДІВНИЦТВА МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ „GROUND CONTROL””

Актуальність теми. На сучасному етапі розвитку Збройні сили України знаходяться у стані, який не дає змогу покращити, прискорити чи раціоналізувати виконання задач у сфері обліку нерухомого майна, оскільки рівень автоматизації, який має вагоме значення для ефективності та раціональності визначення необхідних ресурсів для забезпечення процесів життєвого циклу об’єктів нерухомості, не відповідає вимогам сьогодення. Аналізуючи досвід провідних країн світу та спираючись на діджиталізацію як вектор розвитку країни, визначеного Президентом України, у всіх сферах, зокрема військовій, зроблено висновок у необхідності автоматизації процесів обліку будівництва нерухомого майна Збройних сил України. Виходячи з наведеного та у відповідності до вимог Заступника Міністра оборони України Марценюка О.Е., наприкінці 2019 року робочій групі у складі курсантів від ВІТІ імені Героїв Крут поставлено завдання розробити для потреб ЗСУ Комплекс спеціалізованого програмного забезпечення „Платформа низового моніторингу об’єктів будівництва Міністерства оборони України „Ground control”” (далі комплекс СПЗ) з метою організації процедури моніторингу стану готовності об’єктів житлового та нежитлового фонду. Для забезпечення реєстрації, автентифікації та авторизації користувачів вказаного комплексу необхідна наявність модулю, який реалізує відповідні функції.

Метою дослідження є забезпечення безпеки експлуатації комплексу СПЗ.

Для досягнення мети дослідження у роботі сформульовано наступні **завдання**:

- обґрунтувати необхідність автоматизації сфери контролю та супроводження процесів обліку нерухомого майна Міністерства оборони України;
- проаналізувати принципи забезпечення безпеки корпоративних інформаційних систем та спроектувати структуру модулю;
- розробити програмний модуль реєстрації, автентифікації та авторизації користувача комплексу СПЗ.

Виклад основного матеріалу. Головним завданням модуля є забезпечення реєстрації, автентифікації та авторизації користувачів системи, а також відповідності даного функціоналу принципам забезпечення безпеки корпоративних інформаційних систем. Створений модуль дозволяє користувачам здійснювати вхід, реєстрацію та керування даними облікового запису. Крім того, для зручності користувачів передбачено авторизацію через Google API, завдяки протоколу OAuth2 (протокол авторизації, який дозволяє видати одному сервісу (додатку) права на доступ до ресурсів користувача на іншому сервісі). Аутентифікацію та авторизацію користувачів реалізовано двома технологічними підходами:

1. Збереження ідентифікатора (e-mail користувача) і пароля користувача (який хешується спеціальною функцією криптографічного хешування (SHA-1)) у базі даних MongoDB у відповідності до архітектури інформаційної системи;

2. Виконання авторизації через мережевий сервіс Google за допомогою протоколу OAuth 2.0.

Висновки. Таким чином, в роботі розроблено прикладний програмний інтерфейс модулю авторизації користувача Комплексу спеціалізованого програмного забезпечення „Платформа низового моніторингу об’єктів будівництва Міністерства оборони України „Ground control””. Модуль реалізує унікальний технологічний підхід забезпечення принципів безпеки корпоративних інформаційних систем, який відповідає світовим тенденціям та розроблений з урахуванням досвіду проектування сучасних інформаційних систем.

АНАЛІЗ ПРОГРАМНИХ ДОДАТКІВ ЩОДО ВИРІШЕННЯ ЗАВДАНЬ ТЕХНІЧНОГО АНАЛІЗУ РАДІОТЕХНІЧНИХ СИГНАЛІВ

Актуальність.

В той час коли сучасні радіотехнічні та радіолокаційні засоби знаходяться на етапі стрімкої модернізації і переходять на функціонування в основі швидкодіючих сигнальних процесорів з динамічною реалізацією робочих алгоритмів, процес аналізу радіотехнічних сигналів потребує нових інструментів та підходів. Одним з таких інструментів являються програмні додатки за допомогою яких можливо зробити глибокий і точний аналіз отриманих зразків радіотехнічних сигналів(РТС) та дати оцінку тим чи іншим засобам.

Постановка задачі. Мета. Аналіз існуючих програмних додатків для здійснення ефективного, достовірного та своєчасного визначення частотно-часових параметрів радіотехнічних сигналів.

Основні положення. Використання ефективного програмного забезпечення для проведення аналізу РТС відіграє важливу роль.

На даний частотний аналіз частотно-часових параметрів РТС робиться переважно наступними програмними додатками, такими як:

- спеціалізований програмний додаток(СПД) радіотехнічних станцій;
- програмний додаток SignalsAnalyzer;
- програмний додаток AdobeAudition (раніше випускався під назвою CoolEditPro).

Пропоную розглянути запропоновані програмні додатки за функціональним наповненням, а саме:

- робота з файлами формату wav (IQ-відліки);
- можливість вимірювання часових і частотних параметрів радіотехнічних сигналів в ручному і автоматизованому режимах;
- мінімальна здатність вимірювання тривалості імпульсу;
- наявність та робота з базою даних;
- максимально доступний розмір файлу для проведення аналізу;
- актуальність версії програмного додатку і його підтримка.

Порівняльні результати обраних програмних додатків наведені в таблиця 1.

Таблиця 1.

Назва програмного додатку	Підтримка wav формату	Вимір. f/t параметрів сигналів	Вимір. T_{min} імпульсів	Робота з базою даних	Макс. розмір файлу для аналізу	Остання версія ПД
СПД радіотехнічних станцій	-	f/t + (автом.)	0,3 мкс	+	-	від 2014
ПД SignalsAnalyzer	+	f/t + (ручн.)	1 мкс	-	157 МБ	6.2.6.7 від 2012
ПД AdobeAudition	+	t + (ручн.) f + (візуал.)	1 мс	-	4 ГБ	12.1 від 2018

Висновок. Враховуючи наявний функціонал розглянутих програмних продуктів, можна точно зазначити, що жодна із вищерозглянутих СПД не може забезпечити необхідний функціонал і ефективність аналізу РТС в цілому. Можливо використовувати штатну СПД до станції РТРв поєднанні з ПД SignalsAnalyzer в якості контролю першої, так-як можливості хоч візуально оцінити і порівняти параметри РТС відсутні, але в будь-якому випадку для ведення ефективного аналізу цього недостатньо. Тому є необхідність розробити СПД який буде за своїм функціоналом спроможний виконувати вищезазначені завдання щодо глибокого і точного аналізу РТС.

СПОСІБ РЕЄСТРАЦІЇ ДІАГНОСТИЧНОЇ ІНФОРМАЦІЇ ДЛЯ КОНТРОЛЮ ТЕХНІЧНОГО СТАНУ РАДІОЕЛЕКТРОННОГО ОБЛАДНАННЯ

Актуальність. Розвиток техніки вимагає відповідного розвитку вимірювальних пристроїв для діагностування їх функціонування. На сьогодні все більшого розвитку набувають прилади та засоби, які ґрунтуються на безконтактному методі вимірювання діагностичних ознак технічного стану (ТС) радіоелектронних пристроїв. Одним з найбільш ефективних стали тепловізори. Це складний прилад, який вимірює природне інфрачервоне випромінювання від предметів і перетворює отримані сигнали в теплове зображення.

Постановка задачі. Під час тривалої експлуатації відбувається старіння радіоелектронних компонент (виникає надлишковий опір струму) що викликає помітне підвищення температури в місцях деградації якості. З цієї причини обладнання може виходити з ладу. Спостерігаючи за зонами високої температури в елементах функціонуючої системи (схеми), можна оцінити серйозність виниклих дефектів. Саме тому, використання тепловізорів є найдоцільнішим в даному випадку. Ці прилади дозволяють вирішувати задачі технічної діагностики (визначення фактичного ТС, локалізації несправностей та прогнозування ТС). Так як, під час вимірювання діагностичної інформації фізичний контакт з об'єктом контролю не потрібен, процес контролю може бути здійснено в ході повної експлуатації установки без всякої зупинки технологічного процесу.

Мета. Дослідження полягає в визначенні можливості застосування сучасних засобів реєстрації теплового поля об'єкту контролю (тепловізору) для реєстрації параметрів власного випромінювання радіоелектронних компонентів як основної діагностичної ознаки фізико-хімічних процесів, що відбуваються в цих компонентах під час експлуатації (під час старіння).

Основні положення. Всі об'єкти випромінюють інфрачервону енергію, довжина хвилі якої, залежить від їх температури. Інфрачервоне випромінювання створюється вібрацією і обертанням атомів і молекул усередині тіла. Чим вище температура об'єкта, тим більший їх рух, тобто, більше енергії, що випромінюється в інфрачервоному спектрі. Кількість енергії, що випромінюється від об'єкта на пряму залежить від його температури та коефіцієнту випромінювання. Тепловізори визначають теплове випромінювання (кількість енергії), що надходить від об'єкту контролю та складається з:

випромінювання, що випускається об'єктом
вимірювання; відбитого зовнішнього випромінювання
поглинутого випромінювання.

Компоненти, що розташовані під поверхнею, впливають на розподіл температури на поверхні вимірюваного об'єкту.

За допомогою оптичного приладу, до складу якого входять лінзи прозорі для інфрачервоного випромінювання, теплове випромінювання об'єктів проектується на матрицю чутливу до інфрачервоного випромінювання. Далі інформація з цих датчиків перетворюється з інфрачервоної енергії в електричну напругу. На виході генерується відеосигнал, де різній температурі об'єкта контролю відповідає різний колір зображення. Розмір датчика вказується в пікселях. Кожен піксель датчика є температурною точкою, що відображається на дисплеї. Чим більша роздільна здатність у тепловізора, і чим більшу кількість пікселів містить матриця його екрану, тим точнішим буде вимір фактичної температури об'єкта. Сучасні технології дозволяють розрізняти температуру об'єктів з точністю до 0,05-0,1 К [1].

При визначенні оптимальної відстані до вимірюваного об'єкта і максимального видимого і вимірюваного об'єкта необхідно враховувати: поле зору; найменший видимий об'єкт; найменший вимірюваний об'єкт (область виміру).

Поле зору називається область, видиму тепловізором. Розміри даної площі визначаються можливостями оптики (наприклад 32° , рис. 1а). Для точного вимірювання діагностичної інформації необхідно знати технічні характеристики найменшого видимого об'єкту контролю тепловізора. За допомогою даного значення визначається розмір пікселя в залежності від відстані. Наприклад, з просторовим дозволом об'єктива $3,5$ мрад і відстанню до об'єкта контролю 1 м, найменший видимий об'єкт має сторону пікселя рівною $3,5$ мм і відображається на дисплеї в якості 1-го пікселя. Для отримання точних результатів вимірювання об'єкт контролю повинен бути в 2-3 рази більшим найменшого видимого об'єкта (рис. 1б) [2].

Тепловізійні прилади оснащені пристроями пам'яті для запису отриманого відеозображення, продуктивними мікропроцесорами, що дозволяють здійснювати в режимі реального часу аналіз отриманого в результаті сканування зображення інфрачервоного випромінювання [1,2].

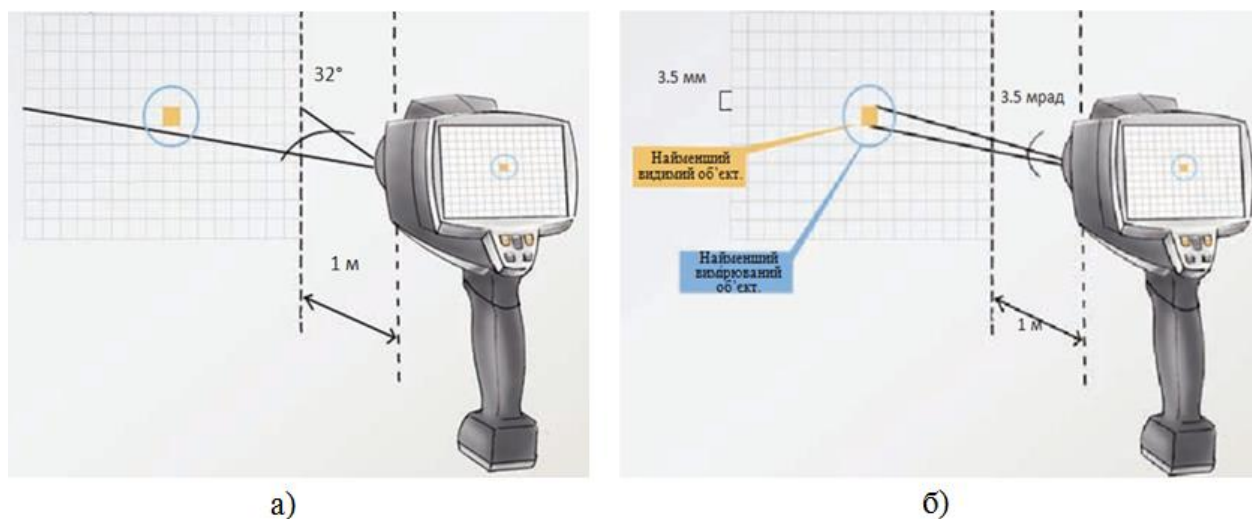


Рис. 1 а) поле зору тепловізора; б) поле зору окремо взятого пікселя

Для ефективного вирішення задач технічної діагностики, особливо для визначення та прогнозування ТС радіоелектронного обладнання доцільним є застосування зазначеного способу реєстрації діагностичної інформації в автономній автоматизованій системі діагностування, оскільки практично усі параметри напівпровідникових приладів і деградаційні процеси, що протікають в них, залежать від температури. При цьому неважливо природа виникнення градієнта температури, важливо те, що відхилення температури від необхідних значень (розрахованих або очікуваних) сигналізує про наявність процесів, що ведуть до відмови.

Висновок. За допомогою даного способу реєстрації діагностичної інформації є можливість в автоматичному режимі без помилок визначати і класифікувати загрозу за мінімальний проміжок часу комплексно підвищуючи ефективність і стійкість реагування на загрозу виходу з ладу всієї системи. Тобто, чим швидше отримана відповідь на питання де виявлено некоректну роботу радіоелектронних компонент, то тим більша ймовірність того, що вся система дійсно вирішує покладені на неї функції та здатна знайти і вирішити проблему, раніше того моменту, як вона призведе до незворотних наслідків.

Таким чином, даний високотехнологічний спосіб реєстрації діагностичного параметру є актуальним та перспективним для подальшого його розвитку та впровадження.

ЛІТЕРАТУРА

1. American Technical Publishers, Inc., Fluke Corporation, и The Snell Group. 2009. – 73 с.
2. Карманное руководство «Термография». Testo AG. 2008. – 56 с. Електронний ресурс: http://www.telesystems.info/files/content_files/Karmannoe_rukovodstvo_po_termografii.pd.

ВАРІАНТ ПОБУДОВИ НЕЧІТКИХ ВІДНОШЕНЬ ДЛЯ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ

Оцінка захищеності інформаційних систем дозволяє визначати, які дії ефективні для мінімізації та попередження загроз. На основі аналізу захищеності можна прогнозувати можливий збиток від реалізації загрози, його оцінку та рекомендувати необхідні дії. Одним з основних факторів використання експертних систем для оцінки захищеності інформаційних систем є можливість збереження та подальшого застосування унікального досвіду експертів. Необхідною умовою розв'язання задач оцінки захищеності є встановлення залежності „загрози-збитки”. У процесі побудови такої залежності суттєву роль відіграє наявність експертних знань про типові збитки та їх ознаки, які часто надаються в нечіткій формі. Тому моделювання таких зв'язків здійснюється із застосуванням теорії нечіткої логіки. Модель системи оцінки захищеності інформаційних систем будується на основі композиційного правила виведення Заде – $B=A \circ R$, в якому носієм інформації є матриця R нечітких відношень „загрози-збитки”, що зв'язує вектор мір значимості загроз A і вектор мір значимості збитків B . Таким чином для розв'язання поставленої задачі необхідно, по-перше, побудувати нечіткі відношення і, по-друге розв'язати систему рівнянь нечітких відношень.

Будемо вважати відомими: $D = \{d_1, d_2, \dots, d_n\}$ – множина загроз, які підлягають порівнянню з точки зору впливу на виникнення збитків; $S = \{s_1, s_2, \dots, s_m\}$ – множина збитків, які означають зміни кількісних або якісних параметрів стану об'єкта.

Необхідно побудувати нечіткі відношення $R \subset D \times S$, тобто необхідно оцінити міру впливу кожної з загроз $d_i, i = \overline{1, n}$, на виникнення кожного з збитків $s_j, j = \overline{1, m}$.

Точні відношення між загрозами та збитками рідко зустрічаються в літературі. Однак часто експерти встановлюють залежності „загрози-збитки” використовуючи інформацію про міру впливу загрози на виникнення збитків у вигляді парних порівнянь типу: *на виникнення збитку A загроза 1 впливає значно більш порівняно з загрозою 2; на виникнення збитку B загроза 1 не впливає або впливає несуттєво порівняно з загрозою 2*. Такі парні порівняння можуть бути використані для побудови матриці нечітких відношень. В цьому випадку збитки розглядаються як нечіткі множини, що задані на універсальній множині загроз. Визначення ступеня належності здійснюється на основі експертної інформації про парні порівняння загроз за допомогою 9-ти бальної шкали Сааті. Перевага такого підходу полягає в тому, що він пристосований як для кількісних, так і до якісних параметрів стану об'єкта. Використання модифікованого методу парних порівнянь Сааті дозволяє отримувати ступені належності у вигляді числа в діапазоні $[0; 1]$, але він не спроможний моделювати можливі невизначеності, а саме неоднозначність порівняльних оцінок і невизначеність через розбіжність в наслідкових частинах експертних тверджень щодо вибору діапазону оцінок. Таким чином необхідно розробити варіант побудови нечітких відношень, який враховує визначені недоліки.

Пропонується варіант побудови нечітких відношень в якому: у випадку, коли джерелом невизначеності є неоднозначність порівняльних оцінок, ступінь переваги одного варіанта над іншим оцінювати деяким діапазоном оцінок; а у випадку, коли джерелом невизначеності є розбіжність в наслідкових частинах експертних тверджень щодо вибору діапазону оцінок отримувати гістограму інтервальних порівняльних оцінок.

Висновки: запропонований варіант побудови нечітких відношень дозволяє оперувати з інтервальними порівняльними оцінками шкали Сааті і враховувати розбіжності експертів при виборі порівняльної оцінки за рахунок побудови гістограми порівняльних оцінок та їх осереднення.

МЕТОД ПОБУДОВИ ШАБЛОНІВ ПОТЕНЦІЙНО НЕБЕЗПЕЧНИХ КІБЕРАТАК

Актуальність. Широке застосування комп'ютерних систем та мереж (КСМ) у різних сферах, наприклад, економічній, військовій, енергетичній, транспортній тощо, суттєво впливає на ефективність діяльності не тільки окремо взятої людини, але й суспільства та держави в цілому. Так, сьогодні найбільшу небезпеку для КСМ становлять кібератаки (КБА). До того ж не тільки збільшується їх кількість, а й зростає технологічна складність таких атак. Це, у свою чергу, призводить до погіршення їх виявлення та нейтралізації, що негативно впливає на рівень захищеності КСМ.

Відомі на даний час технології, покладені в основу функціонування систем інформаційної безпеки, ґрунтуються на використанні сигнатурного методу виявлення КБА. Це, відповідно, призводить до появи так званого „ефекту запізнення”, який виникає через часові затримки, зумовлені технологічною процедурою розроблення потрібного шаблону (сигнатури) КБА тільки після її виявлення та нейтралізації, що суттєво знижує захищеність КСМ від нових потенційно небезпечних атак [3]. У технологічному сенсі сьогодні відбувається комплексування відомих підходів до побудови сигнатур шаблонів атак. Кожен із провідних вендорів антивірусного програмного забезпечення, зокрема, Kaspersky Lab, Panda Security, Intel Security-McAfee, ESET, Dr.Web тощо, тримає в комерційній таємниці підходи до побудови шаблонів атак.

Постановка задачі. Отже, завдання виявлення та нейтралізації потенційно небезпечних КБА на КСМ набуває особливої актуальності та може бути вирішене шляхом створення достовірного методу розроблення шаблону потенційно небезпечних КБА, що забезпечить механізм підвищення захищеності КСМ різного цільового призначення.

Основні положення. Зазвичай будь-яка КБА характеризується наявністю невід'ємних складових, які необхідні для досягнення її мети, а саме [13]:

джерело атаки (суб'єкт атаки) – зловмисник, шкідливе програмне забезпечення, за рахунок якого здійснюється КБА;

наявні в КСМ та її компонентах вразливості та варіанти їх використання;

об'єкт КБА, якими можуть бути ресурси КСМ та її компонентів.

Саме визначивши ці складові, можливо буде з високою ймовірністю стверджувати про проведення КБА на КСМ. Отже, метод розроблення шаблонів потенційно небезпечних КБА повинен бути направлений на визначення їх ключових характеристик і параметрів та містити певні кроки.

Крок 1. Дослідження та аналіз КСМ. Для розроблення шаблону потенційно небезпечної КБА необхідно визначити її клас та множину ресурсів КСМ і її компонентів, які потенційно можуть бути атаковані. З цією метою слід проаналізувати стандартний функціональний профіль захищеності (СФПЗ), реалізований у КСМ. Відповідно до [2] їх кількість варіюється від 6 до 24 для одного СФПЗ. У результаті дослідження СФПЗ КСМ та його мінімальних необхідних послуг безпеки можливо визначити клас потенційно небезпечної КБА та множину ресурсів, які можуть бути атаковані.

Крок 2. Визначення джерел первинних даних для побудови шаблонів потенційно небезпечних КБА. Для опису суб'єкта атаки доцільно використовувати бази даних, які містять у собі шаблони дій зловмисника. Обрані бази даних повинні мати максимальну інформативність про складові КБА. Для опису суб'єкта атаки доцільно використовувати бази даних, які містять у собі шаблони дій зловмисника. Прикладом є база шаблонів КБА САРЕС компанії MITRE [6]. Для обрання з усієї множини відомих баз даних необхідно скористатися двома правилами: мінімальна кількість баз даних, які обираються як джерела первинних даних для розроблення шаблонів потенційно небезпечних КБА, має відповідати кількості її складових; обрані бази даних повинні мати максимальну інформативність про складові КБА.

У результаті отримаємо множину баз даних, які будуть використані як джерела первинних даних для розроблення шаблонів потенційно небезпечних КБА.

Крок 3. Оптимізація вихідних даних, необхідних для побудови шаблонів потенційно небезпечних КБА. Оптимізація вихідних даних здійснюється з метою відбору з усієї множини вхідних даних, необхідних для побудови шаблону потенційно небезпечної КБА, конкретних показників та характеристик, що однозначно будуть її визначати. Оптимізацію параметрів множини вхідних даних, що описують суб'єкт атаки, здійснюють шляхом обрання параметрів, які характеризують дії зловмисника, потенційно можливі для експлуатації обраної вразливості чи здійснення КБА на визначений ресурс [4]. Отже, у результаті виконання третього кроку отримаємо усі необхідні дані для побудови шаблону потенційно небезпечної КБА.

Крок 4. Побудова шаблонів потенційно небезпечних КБА. На четвертому кроці безпосередньо створюють два шаблони потенційно небезпечної КБА на КСМ. Перший – диференційно-ігровий, він описує фізику процесів, що відбуваються в КСМ під час проведення потенційно небезпечної КБА [1]. Другий – фізичний шаблон, що містить у собі повний набір характеристик та параметрів, притаманних цій атаці [5]. Отже, практичне використання диференційно-ігрового шаблону потенційно небезпечної КБА дозволяє вивчати процеси кіберзахисту та кібернападу в КСМ за різних вхідних даних, не проводячи натурального експерименту через його потенційну небезпеку для об'єкта.

Перевагою обраного підходу є застосування ознакового принципу для опису різних класів КБА, який забезпечує опис не тільки відомих на сьогодні класів атак, а й дозволяє розширювати ознаковий простір для опису нових, невідомих і, відповідно, потенційно небезпечних класів.

Висновки. Уперше запропоновано новий метод побудови шаблонів потенційно небезпечних КБА, який, на відміну від відомих, усуває базовий недолік відомих підходів – “ефект запізнення” при створенні сигнатури. В його основу покладено визначення ключових характеристик і параметрів потенційно небезпечної КБА, яке здійснюється на підставі аналізу СФПЗ, реалізованого в КСМ, та джерел первинних даних, які використовуються для побудови шаблонів потенційно небезпечних кібератак.

Перспективним напрямом подальших досліджень є розроблення достовірної методики класифікації потенційно небезпечних КБА на КСМ, для виявлення та нейтралізації атаки, тому що виконання кроків 1-4 запропонованого методу дає змогу встановити лише факт проведення потенційно небезпечної КБА.

ЛІТЕРАТУРА

1. Гришук Р. В. Диференціально-ігрова модель шаблону атаки на Web-сервер. Збірник наукових праць ВІКНУ ім. Т. Шевченка. 2010. № 21. С. 104 – 112.
2. НД ТЗІ 2.5-005-99 „Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу”.
3. Охрімчук В., Гришук, Р. Постановка наукового завдання з розроблення шаблонів потенційно небезпечних кібератак. Безпека інформації, 2015. № 21 (3). С. 276 – 282.
4. Пухов, Г. Дифференциальные преобразования и математическое моделирование физических процессов : монография. Киев: Наук. думка, 1986. 160 с.
5. Охрімчук В. Модель шаблону потенційно небезпечної кібератаки. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник, 2018. № 1 (35), С.30 – 39.
6. Гришук Р. В., Охрімчук В. В., Ахтирцева В. С. Джерела первинних даних для розроблення шаблонів потенційно небезпечних кібератак. Захист інформації, 2016. № 1 (18). С.21 – 29.

к.ф.-м.н. Сеник А.П. (НУЛП)
к.е.н. Білаш О.В. (НАСВ)
к.т.н. Ліщинська Х.І. (НАСВ)
к.ф.-м.н. Войтович М.І. (НАСВ)

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ОРГАНІЗАЦІЇ СИСТЕМ СПЕЦІАЛІЗОВАНИХ КОНСУЛЬТАЦІЙ

Актуальність. На початку ХХІ століття роль інформації в діяльності людини є визначальною: чим більше знань має особа, тим вище цінується як фахівець і співробітник. Інформація в наш час є чи не найважливішим тактичним, стратегічним і управлінським ресурсом поряд з людськими, фінансовими і матеріальними ресурсами. Її створення і використання є необхідною основою розвитку і ефективного функціонування різних сфер суспільного життя, і, перш за все, економіки. А це означає, що не тільки кожній людині стають доступними джерела інформації в будь-якій частині нашої планети, але і генерована нею нова інформація стає надбанням всього людства.

Постановка задачі. В сучасних умовах право на інформацію і доступ до неї має життєву цінність для всіх членів суспільства. Зростаюча роль інформації в різних сферах діяльності людини викликає необхідність надання конкретних точних спеціалізованих консультацій.

Мета. Використання інформаційних технологій для організації ІТ-консалтингу.

Основні положення. ІТ-консалтинг, як і інший вид консалтингових послуг, допомагає вирішити велику кількість завдань. Проте бувають ситуації, коли для відповіді на запитання можуть знадобитися спеціалізовані знання, а саме: організація структури управління виробничими, інформаційними та іншими технологіями; створення корпоративної інформаційної системи для обчислень і комунікацій; пошук і впровадження оптимальних ІТ-рішень; аналіз якості та ефективності технічного обслуговування інформаційних мереж; оптимізація витрат на оновлення програмного забезпечення і устаткування, необхідного для надійної та безперебійної роботи інформаційних технологій; збільшення продуктивності технологічних процесів за рахунок впровадження автоматизованих систем управління; захист корпоративних даних, вибір оптимальної системи для цього і визначення ступеня витрат на захист комп'ютерних і корпоративних мереж; визначення рівня компетентності і продуктивності фахівців; навчання та консультування співробітників та інші завдання. Отже, за допомогою ІТ-консалтингу можна знизити витрати на впровадження інформаційних технологій, отримати професійну підтримку ІТ-фахівців, спростити ряд технологічних процесів і захистити внутрішні мережі від крадіжки даних або витоку інформації.

Для активних користувачів Інтернет відомі ситуації, коли складно знайти шукану інформацію або відповіді на поставлені запитання. Зазвичай, такі ситуації відбуваються тоді, коли для відповіді на запитання можуть знадобитися спеціалізовані знання. У зв'язку з цим створені інформаційні джерела, які не лише можуть використовуватись для пошуку ідей та думок людей щодо певної теми, але також допоможуть у підборі експертів у різних сферах. Для вирішення подібного типу завдань в глобальній мережі Інтернет представлені такі популярні сервіси, як: Google Answers, Madsci, Yahoo! Answers, Stack Overflow, Answers, Quora, Brainly.

Висновки. У зв'язку з посиленням конкурентної боротьби, що зумовлене зростанням невизначеності майбутнього і ризиків, пов'язаних з тим, що витрати на отримання інформації для прийняття рішень неспівмірні як з можливими втратами, так і з здобутками, стає актуальною розробка та впровадження веб-орієнтованого інформаційного ресурсу, що дасть можливість проводити консультації користувача в форматі питання-відповіді, долучати необхідні текстові та медіа файли, а також зберігати інформаційний потік в хмарному середовищі. Такого виду інформаційний ресурс дозволить надання професійного консультування з широкого кола питань освітньої, економічної, фінансової, юридичної та багатьох інших сфер господарської діяльності.

ДОСЛІДЖЕННЯ ТА АНАЛІЗ КАНДИДАТУ НА ПЕРСПЕКТИВНИЙ ПОСТКВАНТОВИЙ ЕЛЕКТРОННИЙ ПІДПИС FALCON

В останні роки було проведено значний обсяг досліджень в області квантових комп'ютерів. Якщо коли-небудь будуть побудовані великомасштабні квантові комп'ютери, вони зможуть зламати багато з використовуваних, у даний час, криптосистем з відкритим ключем. Це серйозно підірве конфіденційність і цілісність цифрових комунікацій.

Тому 20 грудня 2016р. NIST США оголосив конкурс [1], на створення криптографічних алгоритмів з відкритим ключем, які були б стійкими у відношенні як до звичайних комп'ютерів, так і до квантових, створення яких не змусить довго чекати. Криптографічна спільнота, повинна бути готова до цього. Розглядаються як кандидати на алгоритми шифрування/інкапсуляції ключів, так і електронні підписи (ЕП).

На сьогоднішній день відбувається 3-й раунд конкурсу NIST PQC. На 2-му етапі залишили 9 кандидатів ЕП, а саме: CRYSTALS-DILITHIUM, FALCON, GeMSS, LUOV, MQDSS, Picnic, qTESLA, Rainbow та SPHINCS+. Три з них (Dilithium, FALCON, qTeSLA) засновані на стійкості алгебраїчних решіток (Lattice-based), чотири (GeMSS, LUOV, MQDSS, Rainbow) – на основі багатовимірних перетворень (MQ-перетворення), один (SPHINCS+) – на стійкості геш-функції, один (Picnic) – на стійкості геш-функції та блокових потокових шифрів [5].

За результатами досліджень перспективних постквантових криптографічних алгоритмів типу ЕП протягом 2-го раунду конкурсу NIST PQC, було отримано наступні результати – були обрані алгоритми-фіналісти та альтернативні алгоритми. У якості алгоритмів-фіналістів були обрані такі алгоритми ЦП як CRYSTALS-DILITHIUM, FALCON та Rainbow. У якості альтернативних алгоритмів – GeMSS, Picnic та SPHINCS+ [5].

Далі більш детально розглянемо перспективний постквантовий алгоритм ЕП, що входить до переліку алгоритмів-фіналістів – Falcon.

Метою доповіді є дослідження та викладення основних теоретичних відомостей щодо алгоритму ЕП Falcon, а також дослідження стійкості та можливостей алгоритму щодо відомих атак.

Загальний огляд алгоритму ЦП FALCON

FALCON – це алгоритм електронного підпису, представлений у рамках проекту NIST „Постквантова криптографія” [1]. Він був розроблений: Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte та Zhenfei Zhang [2, 5].

FALCON – це решітчаста схема підпису. Назва FALCON походить від перших літер того, на чому базується алгоритм, а саме: Fast Fourier Lattice-based compact signatures over NTRU (Компактні підписи на основі швидкої вибірки Фур'є поверх NTRU) [4]. Докладніше про кожне:

Fast Fourier (Швидке перетворення Фур'є) – реалізація люкової вибірки, яка використовується для генерації коротких векторів. Швидка вибірка Фур'є має оптимальне значення для σ (тобто найкоротше, яке не дозволяє втрачати секретну основу). Достатньо, щоб рівень безпеки і кількість запитів, заданих NIST, брали $\sigma \leq 1,312 \|B\|_{GS}$, що у даному випадку означає $\sigma \leq 1,55\sqrt{q}$. FALCON використовує швидку вибірку Фур'є і генерує вектори для використання в якості підписів [4].

Lattice-based (Криптографія на основі решітки) – заснована на завданні короткого вирішення цілих чисел, основна складна задача, яку використовує алгоритм. Завдання короткого цілочисельного рішення полягає у знаходженні цілочисельних коефіцієнтів до

набору векторів, що складають решітку. Схеми на основі решіток, доволі популярні серед учасників конкурсу. Тому вважається, що решітки володіють квантовою стійкістю [4].

Compact signatures (Компактний підпис). Розробники FALCON хотіли мінімізувати розмір відкритого ключа та розмір підпису: $\|pk\| + \|sig\| = (\text{розмір біта відкритого ключа}) + (\text{розмір біта підпису})$. Так як FALCON був побудований на решітках NTRU, то вони можуть бути замінені будь-якою іншою решітчастою системою [4].

NTRU – вже існуюча система на основі решітки. Основний принцип проектування – компактність. З цієї причини FALCON спирається на клас решіток NTRU; вони поставляються з додатковою циклічною структурою, яка не тільки дозволяє зменшити розмір відкритих ключів у коефіцієнт $O(n)$, але і прискорює багато обчислення, принаймні, в коефіцієнт $O(n/\log(n))$. У NTRU секретний ключ складається з чотирьох многочленів: f, g, F і G , які перевіряють рівняння NTRU: $fG - gF = q \bmod \phi$. Відкритим ключем є поліном, h , такий, що $h = gf^{-1} \bmod(q)$ [4].

BEARZ [3] – FALCON вразливий до атак з вини свого розподілу Гауса, тому при впровадженні для використання в реальному світі, слід враховувати фізичні атаки. Також передбачені можливі контрзаходи, в тому числі і контрзахід „перевірка після підпису”, так як несправний підпис не пройде тест на перевірку відповідності підпису нормам, а також перевірку з нульовим значенням. Більш того, можливо реалізувати метод „Подвійного обчислення”, дорогий, але надійний метод, який передбачає, що злоумисник має доступ до апаратних засобів тільки під час одного з процесів підписання.

Ключове відновлення [4]. Найефективніші атаки виходять із зменшення решітки.

Почнемо з розгляду решітки $(\mathbb{Z}[x]/(\phi))^2 \begin{bmatrix} 0 & q \\ 1 & h \end{bmatrix}$. Після використання решітчастого відновлення, на цій основі, було перераховано всі точки решітки в кулі радіуса $\sqrt{2n}\sigma'$, з центром в основі. Таким чином, з великою часткою ймовірності можна знайти $[g|f]$. Якщо використовувати розмір блоку B , перерахування займає незначний час, якщо $(2n - B)$ – норма Грама-Шмідта більше, ніж $\sqrt{3B/4}\sigma'$. Для найбільш відомого алгоритму редукції решітки, DBKZ, це $(\frac{B}{2\pi e})^{1-n/B} \sqrt{q}$. Тоді легко вивести B і показати, що $B = n + O(n)$, що є найшвидшою асимптотичною атакою. Відзначимо, що задане значення для норми Грама-Шмідта вірно тільки тоді, коли основа спочатку отримана у випадковому порядку, і це необхідно (асимптотично).

Підробка підпису [4] може бути виконана шляхом знаходження в тій же решітці, що і раніше, точки решітки на видаленні, обмеженому β від випадкової точки. Це завдання, також, полегшується шляхом проведення спочатку відновлення решітки на вихідній основі.

При використанні вбудовування та DBKZ, умовою успіху є $(\frac{B}{2\pi e})^{n/B} \sqrt{q} \leq \beta$. Це найкраща атака проти випадкових величин, навіть, якщо мається $B = 2n + O(n)$.

Гібридна атака поєднує у собі алгоритм зустрічі посередині і алгоритм відновлення ключа. Вона була використана з великим ефектом проти NTRU, завдяки вибору розріджених поліномів. Однак тут справа йде інакше, так що її вплив набагато скромніше і врівноважується відсутністю просіювання.

Щільний, високий ранг підрешітки. Останні роботи показали, що коли f, g надзвичайно малі в порівнянні з q , то легко атакувати криптографічні схеми, засновані на решітках NTRU. У FALCON навпаки, беремо f та g не дуже маленькими, в той час як q досить великим: побічний ефект полягає в тому, що це робить нашу схему непроникною для атак на так звані „перевантаження NTRU”. Зокрема, навіть, якби f, g були прийняті за виконавчі, нам довелося б вибрати $q > n^{2.83}$, щоб ця властивість була корисною для криптоаналізу. Наш

великий запас, повинен дозволити, навіть, значні поліпшення цього алгоритму бути неактуальними у нашому випадку [4].

Алгебраїчні атаки. Незважаючи на те, що у FALCON існує багата алгебраїчна структура, не існує відомого способу покращити всі раніше згадані алгоритми по відношенню до їх загальної решітки, еквівалентній більше ніж n^2 . Проте, існують ефективні алгоритми для знаходження не надто дрібних елементів в ідеальних умовах $\mathbb{Z}[x]/(\varphi)$ [4].

СПЕЦИФІКАЦІЯ FALCON

Основними елементами в FALCON є поліноми ступеня n з цілочисельними коефіцієнтами.

У FALCON є три відкритих параметра для аналізу: φ , q та β . Крім того, n відноситься до ступеня поліномів, які використовуються для генерації решіток.

1. Поліном поділу кола $\varphi = x^n + 1$, де $n = 2^k$ $n = 2^k$ – степінь двійки. Відзначимо, що φ – монічний і незвідний.

2. Модуль $q = 12289$. У FALCON, у бінарному випадку $q = 12289$, у троїчному $q = 18433$. Звернемо увагу, що $(\varphi \bmod q)$ ділиться на $\mathbb{Z}_q[x]$.

3. Матеріальна межа $\beta > 0$ обмежена розміром вектора [4].

Генерація ключів для FALCON складається з двох основних етапів: створення поліномів, що заповнюють решітки (вибір випадкових поліномів f, g з допомогою відповідного розподілу, яке дає короткі, але не занадто короткі вектори), і побудова дерева FALCON (рівняння NTRU вирішується для знаходження відповідності F і G).

FALCON має відкритий ключ pk , відповідно до особистого ключа $sk = (f, g, F, G)$ та являє собою поліном $h \in \mathbb{Z}_q[x]/(\varphi)$, такий що: $h = gf^{-1} \bmod(\varphi, q)$. Після генерації f та g , F та G можуть бути обчислені для перевірки рівняння NTRU.

Отримані поліноми потрібно розташувати в форматі секретного ключа. Секретний ключ FALCON складається з B та T , де $\hat{B} = \begin{bmatrix} FFT(g) & -FFT(f) \\ FFT(G) & -FFT(F) \end{bmatrix}$ та FFT яке відноситься до швидкого перетворення Фур'є. T , відомий також як дерево FALCON, є нормалізованою LDL декомпозицією $\hat{B} \times \hat{B}^*$ [4].

За допомогою секретного ключа, sk і повідомлення m , спочатку випадкова $salt$, r генерується. Поєднання r та m , $r \| m$ гешується у нове значення s . Потім, використовуючи свої знання основи секретної решітки (f, g, F, G) , синтаксис виробляє пару коротких багаточленів (s_1, s_2) таким чином, що $s_1 = c - s_2 h \bmod \varphi \bmod q$. Правильно зазначений підпис – s_2 [4]. Перевірка підпису полягає у перезаписі s_1 з гешованого повідомлення s і підпису s_2 , а потім у перевірці того, що (s_1, s_2) є відповідним коротким вектором.

Перевірка підпису може бути виконана повністю за допомогою цілочисельних обчислень по модулю q . Зокрема, оскільки підпис є коротким поліномом s_2 , його елементи у середньому близькі до 0, що дозволяє використовувати спеціальний стислий формат, який зменшує розмір підпису [4].

Для порівняння швидкості генерації ключів, створення та перевірки підпису у різних версіях FALCON, а саме: FALCON-512, FALCON-768 та FALCON-1024 було вирішено використовувати ноутбуки з різними процесорами, один більш високого покоління (Intel Core i5-8265U @1.60GHz) та процесор з гіршими показниками (Intel Celeron CPU B815 @1.60GHz).

Звісно, що у залежності від якості процесора, показники будуть різні. За результатами тестів, найкраще себе показав процесор Intel Core i5-8265U, випередивши свого суперника – Intel Celeron CPU B815, за усіма обраними для порівняння параметрами більше, ніж у 3 рази кожний. Більш детальні результати порівняння показано у таблиці 1 та 2.

Таблиця 1 – Результати ефективності з використанням Intel Core i5-8265U @1.60GHz

Реалізація	Генерація ключа (мс)	Підпис (с)	Перевірка (s)	Розмір відкритого ключа (байти)	Розмір підпису (байти)
FALCON-512	26.02	929.6	8323.09	626	617.37
FALCON-768	41.19	504.7	4782.3	1001	993.94
FALCON-1024	72.28	452.9	4053.4	1247	1233.23

Таблиця 2 – Результати ефективності з використанням Intel Celeron CPU B815 @1.60GHz

Реалізація	Генерація ключа (мс)	Підпис (с)	Перевірка (s)	Розмір відкритого ключа (байти)	Розмір підпису (байти)
FALCON-512	78	352.13	2692.08	626	617.4
FALCON-768	124.03	191.55	1553.28	1000	993.95
FALCON-1024	210.88	170.04	1291.7	1245	1233.16

Алгоритм, що було розглянуто – FALCON, вийшов у другий раунд конкурсу NIST „Постквантова криптографія”, на рівні з іншими алгоритмами електронного підпису CRYSTALS-DILITHIUM, Picnic, qTESLA, Rainbow, SPHINCS, MQDSS, LUOV та GeMSS, обійшовши велику кількість інших кандидатів. А також був обраний до 3-го раунду у якості алгоритму-фіналіста. Алгоритм побудовано на комплексі структур: „Компактні підписи на основі швидкої вибірки Фур’є поверх NTRU” (Fast Fourier lattice-based compact signatures over NTRU): Fast Fourier (Швидке перетворення Фур’є), Lattice-based (Криптографія на основі решітки), Compact signatures (Компактний підпис), NTRU–система на основі решітки.

Розглянуті атаки: BEARZ, підробка підпису, гібридна атака, щільний, високий ранг підрешітки, алгебраїчні атаки, ключове відновлення, на даний момент є найактуальнішими для алгоритмів електронного підпису. Але ЕП FALCON доволі успішно протистоїть цим атакам, тому не має явних проблем з безпекою.

Розробники алгоритму стверджують, що FALCON генерує більше компактних підписів, ніж будь-яка інша відома їм схема. За швидкістю генерації та розміру підпису, перевершує відомі алгоритми RSA та DSA.

За результатами тестування, чим краще буде процесор, тим швидше буде генерація ключової пари, створення та перевірка підпису. Тому для серйозної роботи з алгоритмом, рекомендується мати більш потужний процесор.

ЛІТЕРАТУРА

1. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms, 2016. [Електронний ресурс]. – Режим доступу: <https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms>.
2. FALCON, 2020. [Електронний ресурс]. – Режим доступу: <https://falcon-sign.info/>.
3. McCarthy S. BEARZ Attack FALCON: Implementation Attacks with Countermeasures on the FALCON signature scheme / S. McCarthy, J. Howe, N. Smyth та ін. //, 2019. – Режим доступу: <https://eprint.iacr.org/2019/478>.
4. Prest T. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU / T. Prest, J. Hoffstein, T. Pornin та ін. //, 2020. – Режим доступу: <https://falcon-sign.info/falcon.pdf>.
5. Gorjan Alagic Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8309 / Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone // 22 July 2020. – Режим доступу: <https://doi.org/10.6028/NIST.IR.8309>.

МОДЕЛЬ СЕРВЕРА ВІРТУАЛІЗАЦІЇ НА ОСНОВІ ТЕХНОЛОГІЙ КОНТЕЙНЕРИЗАЦІЇ

На даний час все більше сучасних архітектур використовують хмарний підхід до розгортання своїх сервісів, серверів та інших програмних засобів. Він є досить масштабованим та з певними налаштуваннями може забезпечити надійність збереження та передачі даних. Основною перевагою є відмовостійкість оскільки використання технологій реплікації та кластеризації забезпечує неможливість втрати даних, єдиний спосіб це вихід з ладу фізичного серверу.

Віртуалізація – є частиною хмарних технологій, які на даний час стрімко розвиваються. Більшість сучасних сервісів розгорнуті на віртуальних машинах. Це є досить зручно, адже не потрібно під кожний сервіс виділяти цілий фізичний сервер.

Віртуалізацію можна реалізувати за допомогою як гіпервізора так і контейнерів. В одному випадку на фізичний сервер буде встановлено гіпервізор, а в іншому на певну операційну систему (здебільшого Unix) встановлюється програмне забезпечення для створення контейнерів. Одним із найкращих рішень по контейнеризації є Docker.

Docker – інструментарій для управління ізольованими Linux-контейнерами. Docker доповнює інструментарій LXC більш високорівневим API, що дозволяє керувати контейнерами на рівні ізоляції окремих процесів. Зокрема, Docker дозволяє не переймаючись вмістом контейнера запускати довільні процеси в режимі ізоляції і потім переносити і клонувати сформовані для даних процесів контейнери на інші сервери, беручи на себе всю роботу зі створення, обслуговування і підтримки контейнерів.

Початковий код Docker написаний мовою Go і поширюється під ліцензією Apache 2.0. Інструментарій базується на застосуванні вбудованих в ядро Linux штатних механізмів ізоляції на основі просторів імен (namespaces) і груп управління (cgroups). Для створення контейнерів використовуються скрипти lxc. Для формування контейнера досить завантажити базовий образ оточення (команда `docker pull base`), після чого можна запускати в ізольованих оточеннях довільні програми.

Основною перевагою використання контейнерів для розробки віртуальних машин це є підключення до них, оскільки воно можливе за допомогою SSH з'єднання або за обміном публічних ключів RSA.

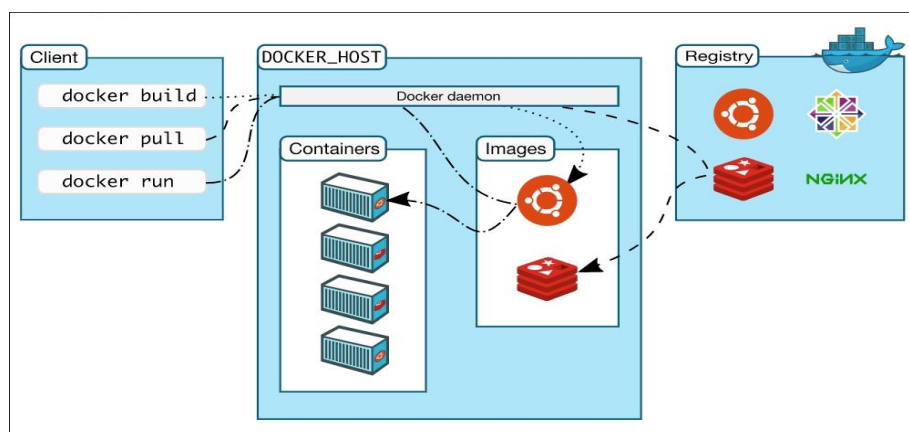


Рис.1. Модель сервера віртуалізації на базі контейнеризатора Docker

Отже, використання контейнерів для створення віртуальних машин забезпечить їх безпеку, зменшить навантаження на фізичний сервер, а так як контейнер є окремим середовищем для розробки, не нанесе нищівних наслідків для сервера.

ПІДСИСТЕМА ВЗАЄМОДІЇ З КОРИСТУВАЧЕМ СИСТЕМИ ОБЛІКУ МАТЕРІАЛЬНИХ ЗАСОБІВ ЛАБОРАТОРІЇ ТЗН ВВНЗ

Актуальність В результаті стрімкого зростання науково-технічного прогресу кожні десять років у світі відбувається подвоєння обсягу наукових знань. Цей чинник викликає істотне збільшення кількості інформації, яка використовується у сфері навчання, і її ускладнення. Виникла об'єктивна необхідність вдосконалення навчального процесу і підвищення його ефективності і якості. Важлива роль у вирішенні цієї проблеми відводиться технічним засобам навчання. Задля рівня навчання та його розвитку і раціональної організації контролю оснащення технічного улаштування засобами навчання аудиторій, кабінетів та відділів було проведено дослідження заради вдосконалення системи обліку матеріальних засобів лабораторії ТЗН ВВНЗ.

З метою покращення ефективності рівня оперативної обробки інформації та швидкої взаємодії між структурними підрозділами впливає, що автоматизації обліку матеріальних засобів лабораторії ТЗН ВВНЗ є важливим питанням, що визначає ефективність системи обліку матеріальних засобів у Збройних Силах України в цілому.

Мета дослідження полягає у вдосконаленні процесу обліку матеріальних засобів лабораторії ТЗН ВВНЗ за рахунок виконання наступних **часткових завдань дослідження**:

аналіз існуючих систем для обліку матеріальних засобів, порівняння їх переваг та недоліків;

аналіз існуючих сучасних технологій для розробки інформаційних систем для обліку матеріальних засобів;

аналіз існуючих веб-технологій для розробки клієнтської частини системи обліку матеріальних засобів

Виклад основного матеріалу. Питання автоматизації обліку матеріальних засобів, як у вигляді автономних систем, так і у складі інформаційних систем управління наразі відпрацьовані достатньо повно. Існують інформаційні системи з функціями обліку матеріальних засобів. Однак запропоновані підходи, в основному, стосуються цивільних організацій, що виробляють, експлуатують і реалізують матеріальні засоби. Аналіз їх можливостей для організації обліку у військових формуваннях не проводився.

Система обліку матеріальних засобів Збройних Сил України відсутня, однак передбачається побудова єдиної інформаційно-аналітичної системи ЗСУ.

Переважна більшість представлених на ринку інформаційних систем мають суттєві недоліки, що значно обмежують можливість їх використання та адаптації до потреб ЗСУ:

- переважна більшість представлених на ринку інформаційних систем мають високу вартість, що особливо актуально, якщо враховувати значну кількість частин та підрозділів;

- інформаційні системи орієнтовані на підприємства промисловості та торгівлі, що мають надлишкову функціональність для частин і підрозділів ЗСУ;

- впровадження інформаційної системи потребує навчання персоналу, що часто здійснюється за додаткову плату;

Висновки. Таким чином, враховуючи зазначені труднощі, було прийнято рішення про розробку власної інформаційної системи для обліку матеріальних засобів лабораторії ТЗН ВВНЗ. При розробці даної інформаційної системи доцільно використовувати такі підходи:

- наявність „дружнього” інтерфейсу користувача, що не потребує спеціальної підготовки користувача;

- модульність – побудова системи у вигляді сукупності взаємопов'язаних модулів;

Реалізація запропонованих підходів забезпечить мінімізацію затрат часу та коштів на розроблення та впровадження.

АНАЛІЗ ФАКТОРІВ ЯКІ ВПЛИВАЮТЬ НА НАДІЙНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Інформаційні системи спеціального призначення (ІССП) використовуються для вирішення завдань державного управління, управління військами і зброєю, екологічно небезпечними та економічно важливими виробництвами тощо. Ці системи функціонують в умовах деструктивних впливів, метою яких є руйнування інформаційних ресурсів, порушення штатних режимів функціонування і, як наслідок, зрив виконання покладених на такі системи функцій. Порушення, припинення або невірне їх функціонування може призвести до серйозних наслідків, усунення яких потребують витрачання значних часових, людських і матеріальних ресурсів. Це визначає необхідність організації захисту ІССП від таких впливів.

За оцінками більшості вітчизняних і зарубіжних фахівців, найбільш вразливим у складі ІССП є програмне забезпечення (ПЗ), причому як системне, так і, більшою мірою, прикладне програмне забезпечення.

Фактори, що впливають на надійність функціонування ПЗ, можна розділити на внутрішні і зовнішні. До внутрішніх джерел загроз надійності функціонування ПЗ можна віднести:

- системні помилки проектування при встановленні цілей і завдань створення ПЗ, при формулюванні вимог до функцій і характеристик вирішення завдань, визначенні умов і параметрів зовнішнього середовища, в якому застосовується ПЗ;

- алгоритмічні помилки розробки при безпосередній специфікації функцій програмних засобів, при визначенні структури і взаємодії компонентів комплексів програм, а також при використанні інформації з баз даних;

- помилки програмування в текстах програм і описах даних, а також у вихідній і результуючій документації на компоненти і ПЗ в цілому. У процесі налаштування основна частина помилок в програмах виявляється і усувається, проте завжди є ризик пропуску декількох помилок. Будь-яке налаштування ПЗ може показати наявність помилок, але не може довести їх відсутність. В процесі тестування і налаштування ПЗ практично неможливе виконання абсолютно повних перевірок, що гарантують відсутність неперевіраних компонентів програми і повне виявлення всіх можливих помилок. В результаті в ПЗ завжди існує певна кількість невиявлених помилок;

- недостатню ефективність використовуваних методів і засобів оперативного захисту програм і даних від збоїв і відмов та забезпечення надійності функціонування ПЗ в умовах випадкових негативних впливів.

Зовнішніми дестабілізуючими факторами є:

- помилки оперативного та обслуговуючого персоналу в процесі експлуатації ПЗ;

- спотворення в каналах мереж зв'язку інформації, що надходить від зовнішніх джерел, а також неприпустимі для конкретної інформаційної системи характеристики потоків зовнішньої інформації;

- збої і відмови в апаратурі обчислювальних засобів;

- зміни складу і конфігурації комплексу обладнання інформаційної системи за межі, які перевірені при випробуваннях або сертифікації і відображені в експлуатаційній документації.

Повністю виключити всі ці фактори неможливо. Тому необхідно розробляти засоби і методи зменшення їх впливу на надійність ПЗ. Ступінь впливу всіх внутрішніх дестабілізуючих чинників і деяких зовнішніх на надійність ПЗ найбільшою мірою визначається якістю технологій проектування, розробки, супроводу та документування ПЗ.

ROS-M ТА ПРОГРАМНА АРХІТЕКТУРА AGVRA.

Поширення роботизації поля бою робить актуальним завданням стандартизацію наземних безекіпажних комплексів (UGV) як у питаннях їх архітектури, так і програмного забезпечення. Відсутність достатнього досвіду у цій сфері серед вітчизняних фахівців доцільно компенсувати вивченням та врахуванням позитивного світового набутку, зокрема напрацювань експертів НАТО.

Метою доповіді є обґрунтування використання при розробці безекіпажних сухопутних платформ концепції операційної системи ROS-M та архітектури AGVRA як альтернативи стандартизованих в НАТО архітектурі транспортних засобів NGVA.

ROS-M (Robotic Operating System – Military) – це програмна екосистема для військових роботизованих та автономних систем (RAS) [1], заснована на відкритій операційній системі роботів (ROS). Слід зазначити, що ROS-M не є операційною системою у звичайному розумінні. Це система розробки та комунікаційне середовище, яке забезпечує у тому числі 3D-моделювання і відповідну візуалізацію результатів. ROS-M почали розробляти у 2016 р. під спонсорством TARDEC, у 2017 р. було створено прототип системи, який був викладений на сайті di2e.net з обмеженим доступом за відповідною реєстрацією. На даний момент для ROS-M на сайті di2e.net створено захищений репозиторій та реєстр із підтримкою спеціальних інструментів для військових застосувань та компонент для військових організацій, що використовують проміжне програмне забезпечення (Middleware) ROS у своїх розробках. Зазначений репозиторій містить як відкрите програмне забезпечення, так і пропріетарне та таке, що є власністю лише уряду США.

Важливо, що ROS-M забезпечує довірену спільноту урядових та галузевих розробників програмного забезпечення засобами для колективного накопичення, обслуговування і використання об'єднаних об'єктів багаторазових, сумісних із ROS програмних пакетів та модулів, придатних для військових застосувань.

До складу ROS-M входять інструменти, що базуються на відкритій структурі ROS, такі як: реєстр для пошуку та каталогізації, що стосується оборонного програмного забезпечення, сумісного з ROS, та стандартизований пакет інструментів кібербезпеки для виявлення вразливостей програмного забезпечення. Ці можливості дозволяють урядовим і галузевим розробникам та інтеграторам легко виявляти й оцінювати існуючі програмні пакети та модулі, які вони можуть використовувати для створення прототипів і виготовлення військових роботизованих автономних систем (RAS), за менший час, з меншим ризиком та з меншими витратами.

За великим рахунком, військову версію операційної системи ROS-M можливо розглядати як основу для відповідного стандарту НАТО у сфері UGV, оскільки багато країн вже використовують де-факто відкриту систему ROS, і такий стандарт НАТО сприяв би взаємосумісності через краще і широке впровадження екосистеми. Разом з тим, доступ до поточного реєстру ROS-M мають лише міністерство оборони та оборонні підрядниками США. Це представляло проблему для НАСА разом з іншими цивільними розробниками з боку США. Для вирішення вказаної проблеми планується створити дублікат реєстру, відкритого для інших урядових установ та підрядників США, ніж лише міністерство оборони. Деякі пакети можуть не ділитися між двома реєстрами, але експерти вважають, що більшість з програмних напрацювань можуть бути спільними. Вивчається можливість зробити щось подібне і для реєстру НАТО, який в подальшому буде доступний державам-членам НАТО та їх підрядникам. До речі, аналогічний реєстр було б доцільно започаткувати й в Україні.

У 2020 р. тривало удосконалення ROS-M, інтеграція її з ROS 2.0 (планується випуск нової версії ROS-M 2.0.), профілем взаємосумісності (IOP) UGV та програмною

архітектурою AGVRA. Крім того, важлива увага приділяється поліпшенню кіберзахисту. Серед перспективних напрямів реалізації ROS слід вказати її інтеграцію зі службою поширення даних DDS для групового управління кількома роботами. Таке завдання є досить серйозним викликом, однак його вирішення буде лише питанням часу.

Стосовно згаданого профілю взаємосумісності UGV базовим документом для Robotic Autonomous Systems - Ground (RAS-G) є STANAG 4818/AEP-4818 Unmanned Ground Vehicle Interoperability Profiles (IOP). Відкритий характер зазначеної союзницької публікації дозволяє рекомендувати її для запровадження в Україні. Разом з тим робота з удосконалення AEP-4818 триватиме й після її ратифікації у 2021 р. Зокрема, актуальним завданням є управління через VPN роботизованими платформами у складі людино-роботизованих команд (Manned/Unmanned Teaming, MUMT).

Стосовно AGVRA (Autonomous Ground Vehicle Architecture) слід зауважити, що після офіційної публікації стандарту на архітектуру NGVA (Next Generation Vehicle Architecture) експерти НАТО певний час вважали за доцільне використання NGVA в якості перспективної архітектури для UGV. Однак у 2019 р. відбулася зміна орієнтирів у позиції експертів, оскільки за останніми оцінками, проведеними фахівцями U.S. Army Combat Capabilities Development Command (CCDC) Ground Vehicle Systems Center (GVSC) (колишній Центр досліджень, розробок та інженерінгу бронетанкової техніки США (TARDEC)) [1, 2], NGVA [3] та її модель даних є досить надмірною і складною для невеликих UGV. Це, окрім технічних проблем, призводить до невиправданого збільшення вартості як самих UGV, так і їх розробки. Тому для невеликих за розміром тактичних UGV в якості альтернативної програмної архітектури розглядається започаткована в США архітектура автономних наземних транспортних засобів AGVRA.

Програмна архітектура AGVRA вперше згадується у публікаціях фахівців США щодо UGV у 2015 р. (AGVRA 1.0). В кінці 2017 р. вона була поновлена до версії AGVRA 2.0, а у 2019 р. – до версії AGVRA 3.0.

На даний момент відпрацьовано систему поглядів на архітектуру (Operational View, Capability View і т.д.), узагальнено випадки її використання (Use Cases), ведеться робота над відповідним програмним забезпеченням. Очікується, що у майбутньому американська відкрита архітектура бойових транспортних засобів VICTORY (*Vehicular Integration of C4ISR/EW InTerOpeRabilitY*) теж матиме інтерфейс з AGVRA. Взагалі за планами експертів США розробка AGVRA триватиме до 2026 р. Однак слід вказати на очікування певних переваг від її впровадження ще до завершення зазначеного терміну. Разом з тим, необхідно зробити висновок, що несумісність VICTORY з архітектурою транспортних засобів NGVA робить проблематичним забезпечення взаємосумісності AGVRA з NGVA. Вирішення цього завдання буде теж відтерміноване у часі, хоча передумови для його спрощення закладаються Асоціацією MILVA шляхом розробки нового тому настанови щодо NGVA стосовно апаратних шлюзів. У разі виконання їх на основі смарт-технологій програмної реконфігурації, запропонованої автором, цілком можливо буде оперативно узгоджувати інтерфейс NGVA з AGVRA завдяки адаптивній зміні програмно-апаратних налаштувань.

ЛІТЕРАТУРА

1. Слюсар, В.І. Нова система досліджень і розробок сухопутних військ США. // Озброєння та військова техніка. – №3. – 2019. – С.123 – 128.
2. Слюсар, В.І. (2019). Ключові суб'єкти НАТО з розвитку наземних роботизованих комплексів (UGV).// Науково-практична конференція „Застосування Сухопутних військ Збройних Сил України у конфліктах сучасності”. – 14 – 15 листопада 2019 р. – Львів: Національна академія Сухопутних військ ім. Гетьмана Петра Сагайдачного, 2019. – С. 70.
3. Слюсар В.І. Концепція архітектури транспортних засобів як мережі мереж.//Збірник матеріалів XII науково-практичної конференції „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 р.). – Київ. – С. 218 – 219.

ТЕНЗОРНО-МАТРИЧНІ ОСНОВИ ТЕОРІЇ ШТУЧНОГО ІНТЕЛЕКТУ

Ефективна інтеграція систем штучного інтелекту (AI) та великих обсягів даних стикається з проблемою пошуку швидкодіючих обчислювальних алгоритмів, які дозволяють вирішувати завдання обробки багатовимірних інформаційних масивів у реальному масштабі часу. Особливу гостроту цій проблемі надає парадигма, що запанувала на даному етапі розвитку побудови подібних систем на основі глибоких загорткових нейромереж і передбачає, зокрема, формування згорток великої розмірності. Хмарні механізми доступу до таких мегаструктур інспірували не тільки масове впровадження систем стільниковому зв'язку 5-го покоління для вирішення проблем скорочення часу передачі великих масивів даних, але й сприяли початку розробок систем зв'язку 6G, у тому числі на основі квантових мереж. Разом з тим, підвищення швидкості передачі даних є лише одним з аспектів концепції наближення сервісу AI до споживача. Іншою стороною проблеми залишається необхідність здешевлення обчислювальних технологій, що лежать в основі алгоритмів обробки даних систем штучного інтелекту й машинного навчання.

Через це останнім часом зусилля багатьох дослідників активізувалися за напрямом адаптації розробленої в алгебрі тензорно-матричної теорії під потреби систем машинного навчання в інтересах компактної формалізації аналітичного опису алгоритмів функціонування AI.

Одним з таких напрямів є використання торцевого добутку матриць, запропонованого автором в 1996 р. [1]. У відношенні двох матриць із однаковою кількістю рядків суть його зводиться до множення кожного елемента окремо взятого рядка лівої матриці на відповідний рядок правої. Такий підхід одержав визнання серед закордонних фахівців, підтвердженням чому стали публікації Томаса Ейле (Thomas D. Ahle) зі співавторами, присвячені аналізу ефективності так званого тензорного скетчу [2].

Тензорний скетч як метод зменшення розмірності інформаційних просторів був запропонований в 2013 р. і використовується в алгоритмах обробки великих даних, статистиці, машинному навчанні для зниження розмірності масивів даних на основі їх векторного представлення у вигляді тензорної структури. Такий скетч може бути використаний для прискорення білінійного об'єднання в нейронних мережах, зменшення кількості змінних, необхідних для реалізації пулінга і є наріжним каменем багатьох числових алгоритмів лінійної алгебри.

Суттєво, що операцію формування тензорного скетчу можна представити у вигляді добутку деякої матриці великої розмірності й тензорного добутку векторів вихідних даних. В основі варіанта зниження відповідних обчислювальних витрат, запропонованого Томасом Ейле й ін., лежить використання відносно тензорного скетчу властивості зазначеної операції торцевого добутку, що дозволяє звести матрично-тензорний добуток до поелементного множення Адамара. Із цією метою досить представити вихідну матрицю тензорного скетчу у вигляді торцевого добутку матриць меншої розмірності. В результаті вихідний формат скетчу зводиться до добутку Адамара наборів невеликих матриць із елементами 1 і -1 або гауссових матриць Джонсона-Лінденштрауса й субвекторів, що утворювали спочатку тензорний добуток з набору векторів даних.

Оскільки класичні операції матрично-векторних множень здійсненні за лінійний час, перехід до нового формату подання тензорного скетчу на основі властивості торцевого добутку дозволяє виконати множення на вектори з тензорною структурою набагато швидше, чим формувався б вихідний вираз. Для тензорів високого порядку економія в кількості операцій множення може бути досить значною. При цьому важливо, що подібне перетворення при великій кількості матриць у складі торцевого добутку задовольняє лемі Джонсона-Лінденштрауса про малі викривлення вихідних даних великої розмірності при побудові їх проєкцій.

Для згорткових нейромереж важливо, що така концепція може бути поширена на випадок формування швидкого перетворення Фур'є (БПФ) від тензорного скетчу у вигляді векторної згортки в часовій області. У результаті, перехід до спектрального представлення дозволяє замінити зазначену згортку еквівалентною операцією множення торцевого добутку БПФ-матриць у комбінації з підматрицями тензорного скетчу на кронекерівський добуток векторів даних. Це забезпечує заміну ресурсномістких обчислень простим у реалізації поелементним добутком Адамара.

Томас Ейле також запропонував підвищити за допомогою торцевого добутку продуктивність швидкого перетворення Джонсона-Лінденштрауса (FJLT) за методом SHD. З цією метою він використовував в якості випадкової матриці S , складеної з рядків, що утворюють одиничну матрицю, торцевий добуток двох аналогічних матриць меншої розмірності. Як наслідок перетворення FJLT від тензорного добутку векторів звелось до добутку Адамара. З тим же успіхом даний підхід може бути розповсюджений на інші версії FJLT – субдискретизоване рандомізоване перетворення Фур'є (Subsampled Randomized Fourier Transform) і вдосконалені модифікації субдискретизованого рандомізованого перетворення Адамара (subsampled randomized Hadamard transform). Загальна методологія розпаралелення такого роду перетворень на потоки меншої розмірності полягає в тому, що вибіркова матриця відліків S представляється торцевим добутком двох матриць із меншою кількістю елементів. У підсумку весь вихідний добуток при множенні матриці проєкції на тензорний добуток векторів розщеплюється на добуток Адамара.

Слід зазначити, що в контексті згаданої властивості торцевого добутку ідея переходу від вихідного матричного проєктора до добутку Адамара, що оперує матрицями малої розмірності, була використана в 2010 році для розв'язку завдання диференціальної приватності (differential privacy) при доступі до баз даних. Крім того, аналогічні обчислення були застосовані для реалізації ядерних методів AI.

Разом з тим, перераховані підходи торкаються лише верхівки айсберга всієї сукупності можливих застосувань апарата торцевих добутків матриць як основи тензорно-матричної теорії штучного інтелекту. Заслуговує на увагу, наприклад, узагальнення розглянутих варіантів розв'язку завдання зниження розмірності даних на основі використання запропонованого автором блокового варіанта торцевого добутку матриць (БТП) [1], оскільки такі блокові структури є, як відомо, зручною формою запису багатовимірних тензорів. При певних форматах матричних блоків застосування БТП також зводиться до Адамарового добутку матрично-векторних структур або, у більш загальному випадку, - до поблочної суми добутків Адамара. Це дозволяє перетворювати багатоканальні ієрархії згорткових нейромереж до більш простих у навчанні структур.

Компактно формалізувати процес зважування аналізованих масивів даних на вході нейромережі пропонується на основі проникаючого торцевого добутку [3], який зводиться до поелементного множення лівої матриці на погоджені за розміром блоки правої блокової матриці. У випадку мультизгорткових нейромереж складної ієрархії доцільно використовувати узагальнений торцевий добуток і його блокову версію [3].

Розглянуті підходи можуть бути реалізовані програмно або на апаратному рівні в нейрочипах і будуть сприяти впровадженню AI на тактичному рівні.

ЛІТЕРАТУРА

1. Слюсар В.И. Торцевые произведения матриц в радиолокационных приложениях// Известия высших учебных заведений. Радиоэлектроника. – 1998. – Том 41, № 3. – С. 71 – 75.
2. Ahle, Thomas. Almost Optimal Tensor Sketch. Researchgate (3 сентября 2019).
3. Слюсар В.И. Обобщенные торцевые произведения матриц в моделях цифровых антенных решеток с неидентичными каналами.//Известия высших учебных заведений. Радиоэлектроника. – 2003. – Том 46, № 10. – С. 15 – 26.

СТРАТЕГІЯ СТАНДАРТИЗАЦІЇ У СФЕРІ UGV

Аналіз досвіду держав-членів НАТО свідчить про необхідність побудови стратегії стандартизації наземних роботизованих комплексів та автономних систем зброї із штучним інтелектом на основі поетапного вирішення відповідних проблем.

Метою доповіді є обґрунтування змісту та послідовності етапів реалізації національної стратегії стандартизації у сфері безпілотних сухопутних платформ.

На першому етапі пропонованої стратегії найвищий пріоритет необхідно надати відповідному оновленню діючих оперативних стандартів з внесенням змін до доктринально-організаційних складових національної системи DOTMLPFI. Паралельно має бути розпочата розробка ключових технічних стандартів, перш за все таких, що стосуються випробувань систем UGV. Річ у тім, що чимало компаній вже розробили зразки безпілотних платформ, і необхідно відібрати з них найбільш придатні до військового використання та виявити такі, що заслуговують подальшого удосконалення.

Офіційне прийняття технічних стандартів має стати змістом другого етапу реалізації зазначеної стратегії. При цьому одночасно слід продовжити затвердження нових операційних нормативів, розуміння потреби в яких виникло у контексті технічної стандартизації. Основними напрямками подальшої нормотворчої діяльності у технічній сфері має бути розробка загальних стандартів архітектури, інтерфейсів, інформаційного обміну, взаємосумісності з іншими пілотованими та безпілотними платформами, у тому числі UGV з БПЛА. Технічна стандартизація має забезпечити здатність UGV „підключатися” до існуючих та майбутніх мереж C2/C4I, забезпечити безпеку експлуатації UGV, зокрема у кібернетичній сфері. В той же час слід врахувати, що стандарти певним чином перешкоджають інноваціям, і тому необхідно періодично змінювати вже прийняті оперативні та технічні стандарти, підлаштовуючи їх під розвиток технологій. Цей трудомісткий процес повинен розпочатися в рамках третього етапу стандартизації.

Крім того, на національному та міжнародному військових рівнях важливо чітко розмежувати велику кількість визначень і термінів для роботів/робототехніки, безпілотних систем і пов'язаних з ними систем/компонентів та атрибутів, щоб уникнути загальної плутанини. Цей процес слід також завершити відповідним стандартом.

Необхідно буде запровадити нові нормативи для операторів та програмістів, затвердити специфічний набір професійних навичок для експертів у галузі безпілотних систем.

Хоча існують численні переваги використання безпілотних систем для забезпечення підтримки військ, слід також враховувати виклики, які будуть пов'язані з можливим продовженням поширення експлуатації різних типів таких систем. Тому для успішних операцій з логістичної підтримки вирішальною буде розробка стандартів щодо джерел живлення UGV, їх зброї, боєприпасів, обладнання та обслуговування.

Увесь зазначений комплекс завдань має бути спланований та скоординований з метою формування системи систем стандартів [1] як кінцевого завдання стратегії стандартизації. Тільки такий підхід дозволить уникнути хаотичності та фрагментарності у розробці стандартів, забезпечить ефективність та синергію їх впровадження в інтересах розвитку спроможностей UGV і оснащених ними військових підрозділів в складній ієрархії місій та перспективних сценаріїв бойових дій.

ЛІТЕРАТУРА

1. Слюсар В.І. Щодо стратегії формування системи систем стандартів НАТО. // 36. матеріалів V міжнародної науково-практичної конференції „Проблеми координації воєнно-технічної та оборонно-промислової політики в Україні. Перспективи розвитку озброєння та військової техніки”. – Київ, 11 – 12 жовтня 2017 р. – С. 84 – 86.

КОНЦЕПЦІЯ КІБЕРБЕЗПЕКИ ЗБРОЙНИХ СИЛ США

Військово-політичне керівництво США першим почало розглядати кібернетичний простір як нову сферу ведення бойових дій поряд з наземною, морською та повітряно-космічною сферами. У травні 2009 р. апаратом Білого дому в кооперації з комісією з питань кібербезпеки Центру стратегічних та міжнародних досліджень була підготовлена концепція „Інформаційна перевага”, згодом використана в документі про стратегію розвитку збройних сил (ЗС) США “Єдина перспектива – 2020”.

Основними принципами нової стратегії комплексної кібербезпеки в США є наступні положення:

- створення умов для подальшого розвитку кіберпростору з акцентом на вдосконалення та розширення широкосмугових мереж;
- розподіл відповідальності за кібербезпеку з одночасною тісною взаємодією між федеральними відомствами, місцевою владою та приватним бізнесом;
- створення ефективної скоординованої системи розподілу інформації та реагування на інциденти;
- заохочення та фінансування впровадження інноваційних розробок в галузі кібербезпеки;
- удосконалення підготовки фахівців з кібербезпеки, які повинні володіти інструментами оборонного та наступального призначення.

У 2009 р. у США сформоване нове командування бойових дій у кіберпросторі USCYBERCOM, яке перебуває в структурі об'єднаного стратегічного командування США USSTRATCOM і є основним органом управління бойовими діями в кіберпросторі Збройних сил США. Основне призначення USCYBERCOM – координація захисту комп'ютерних мереж США та організація наступальних операцій у кібернетичному просторі.

Ключовими завданнями командування USCYBERCOM у кіберпросторі є:

- забезпечення захисту інформаційних мереж міністерства оборони США;
- координація взаємодії профільних структур міністерства оборони США в сфері кібербезпеки;
- представництво інтересів міністерства оборони США з питань кібербезпеки на національному рівні;
- надання сприяння та участь у загальнонаціональних заходах щодо забезпечення безпеки в кіберпросторі, проведених під керівництвом інших федеральних відомств США;
- оперативне управління виділеними видами ЗС США силами та засобами ведення бойових дій у кіберпросторі;
- координація планування, розробка та ведення розвідувальних, оборонних і наступальних операцій у кіберпросторі.

Поставлені завдання командування USCYBERCOM вирішує у взаємодії з агентством національної безпеки (АНБ) і управління інформаційних систем (УІС) міністерства оборони США. Зазначені органи міністерства оборони в рамках вирішення завдань забезпечення кібербезпеки та ведення бойових дій у кіберпросторі відповідають за своєчасне надання для USCYBERCOM розвідувальної інформації АНБ та технічної підтримки УІС.

В організаційно-штатній структурі USCYBERCOM використовувалася модель об'єднаного бойового командування, що включає в себе кіберкомандування родів збройних сил, що, на думку вищого військового керівництва США, дозволяє найбільш ефективно задіяти можливості всіх видів збройних сил США та враховувати їхні інтереси при веденні загальновійськових операцій. Наведений досвід збройних сил США з побудови системи кіберзахисту може бути використаний під час створення ефективної системи кіберзахисту в інтересах сектору безпеки та оборони України.

РОЗПОДІЛ ЧАСТОТНОГО РЕСУРСУ СУЧАСНИХ ШИРОКОСМУГОВИХ СТАНЦІЙ В ТАКТИЧНІЙ ЛАНЦІ УПРАВЛІННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ

Початок бойових дій на сході України сформував потребу в сучасних засобах зв'язку. Перед Військами зв'язку Збройних Сил України постали складні питання які потребували негайного вирішення. Одним з таких питань було швидке нарощування системи зв'язку сучасними радіорелейними засобами. Вирішенням цієї потреби було використання цивільних засобів зв'язку таких як станції широкосмугового доступу типу Ubiquiti та MikroTik. Зазначене рішення дало змогу суттєво та у відносно короткі терміни наростити спроможності системи зв'язку. З використанням станцій широкосмугового релейного зв'язку були розгорнуті лінії прив'язки, лінії прямого зв'язку, та елементи польової опорної мережі.

В подальшому шляхом адаптації цивільних технологій на постачання Військ зв'язку Збройних Сил України було поставлено радіорелейні станції Р-425, Р-402, що дозволило частково впорядкувати різноманіття засобів зв'язку.

Проте з позитивними сторонами переходу Військ зв'язку на сучасні засоби зв'язку таких як збільшення пропускної спроможності інтервалів, покращення завадозахищеності та розвідзахищеності сигналу було отримано ряд негативних моментів таких як неможливість в більшості випадків побудувати лінії прямого зв'язку за класичною схемою (потреба в додаткових пунктах ретрансляції), організація радіорелейного зв'язку тільки в зоні прямої видимості, прив'язка до висотних об'єктів місцевої інфраструктури таких як мережа теле-радіо компаній.

Велика насиченість зазначеними широкосмуговими радіорелейними засобами та застарілими підходами щодо організації зв'язку призвели до виникнення ряду проблемних питань, які можливо умовно розділити на адміністративні та технічні.

Адміністративними проблемами в організації зв'язку є:

- відсутність інформації (геоінформаційної бази даних) щодо об'єктів цивільної інфраструктури таких як вишки операторів зв'язку та теле-радіо компаній;
- не внесені зміни в керівні документи щодо організацій радіорелейного зв'язку;
- не ведеться розподіл частотного ресурсу на домінуючих висотах (об'єктах місцевої інфраструктури).

Технічними проблемами в організації (забезпеченні) зв'язку є:

- відсутнє програмне забезпечення управління системою зв'язку що прийнята на озброєння (постачання);

- відсутні технічні засоби для сканування частотного діапазону в місцях розгортання радіорелейних засобів.

- відсутність вимог щодо розгортання технічних засобів у відношенні електромагнітної сумісності;

- відсутність вимог щодо якості каналів зв'язку;

- відсутність засобів вимірювання.

Для вирішення зазначених проблемних питань пропонується: внесення змін в нормативні документи з організації зв'язку (Настанову зі зв'язку, Настанову з радіорелейного та тропосферного зв'язку), проведення випробувань та в подальшому формування технічних умов щодо розгортання засобів зв'язку, здійснення технічного переоснащення вимірювальними приладами (засобами) зв'язку, впровадження засобів автоматизації процесів бойового застосування Військ зв'язку.

СПОСОБИ ПІДВИЩЕННЯ ЕНЕРГЕТИЧНОЇ ЕФЕКТИВНОСТІ ЗАСОБІВ ВІЙСЬКОВОГО РАДІОЗВ'ЯЗКУ З ПІДТРИМКОЮ ТЕХНОЛОГІЇ МІМО

Останні роки пов'язані зі стрімким розвитком систем безпроводового зв'язку (СБЗ), що одночасно забезпечують високу швидкість та достовірність передачі великих обсягів інформації. Тому головним завданням таких СБЗ при обмежених просторово-частотно-енергетичних ресурсах є підвищення їх спектральної (СЕ) і енергетичної (ЕЕ) ефективності. На теперішній час найбільш продуктивним способом забезпечення високих ЕЕ та СЕ сучасних СБЗ є технологія багатоантенних систем МІМО (Multiple Input – Multiple Output). За твердженням провідного фахівця в галузі цифрових телекомунікацій Р. Кальдербанка, додаткове використання просторового ресурсу на базі сучасних гнучких та універсальних способів просторово-часового кодування сигналів у багатоантенних системах МІМО дозволяє істотно покращити можливості та умови обміну ЕЕ на СЕ.

Ефективність МІМО залежить від кількості передавальних та приймальних антен. Основними обмеженнями щодо застосування великої кількості антен є вимоги до компактності мобільних терміналів, а також забезпечення мінімального рівня просторової кореляції замирань між сигналами. Слід зауважити, що значний рівень просторової кореляції призводить до зменшення пропускної спроможності каналу зв'язку та здатний звести до нуля всі переваги МІМО, тому кількість антенних елементів приймача/передавача найчастіше не перевищує двох-чотирьох.

Технологія МІМО стала невід'ємною частиною практично всіх сучасних стандартів безпроводового зв'язку: Long-Term Evolution (LTE) і LTE-Advanced (LTE-A), IEEE 802.16 WiMAX та IEEE 802.11 Wi-Fi та базою для СБЗ наступних поколінь.

У каналах МІМО використовуються такі базові способи просторово-часового блочного кодування (Space-Time Block Coding, STBC): ортогональні (Orthogonal, OSTBC) та неортогональні (Non-Orthogonal, NOSTBC). Способи OSTBC дозволяють значно підвищити завадостійкість передачі інформації за рахунок просторового рознесення сигналів (Spatial Diversity, SD), проте вони не є оптимальними за показником СЕ. Способи NOSTBC забезпечують істотне збільшення швидкості передачі інформації шляхом просторового мультиплексування сигналів (Spatial Multiplexing, SMX), однак вони потребують удосконалення в частині SD. Новими варіантами застосування МІМО, що з'явилися протягом останнього десятиліття, є формування діаграми спрямованості (Beamforming, BF) та просторова модуляція сигналів (Spatial Modulation, SM). Спосіб BF є ефективним у каналах з просторовою кореляцією, а SM є енергетично ефективнішою альтернативою способу SMX за сприятливої завадової обстановки та низьких-середніх показниках СЕ.

Найвідомішим OSTBC для двох передавальних та довільної кількості приймальних антен є код Аламоуті, використання якого дозволяє наблизитись до повної пропускної спроможності MISO 2×1 (Multiple Input – Single Output). Коди NOSTBC дозволяють істотно підвищити СЕ, проте характеризуються низькою ЕЕ, а також високою обчислювальною складністю практичної реалізації приймача. Серед NOSTBC широко застосовується код VBLAST (Vertical-Bell Laboratories Layered Space-Time), що забезпечує передачу інформаційних потоків по потенційно незалежним паралельним просторовим каналам (SMX) за умови некорельованості шляхів між кожною парою приймально-передавальних антен. У сучасних стандартах безпроводового зв'язку використовуються ортогональні та неортогональні типи породжувальних матриць просторово-часових кодів. Наприклад, у WiMAX коди Аламоуті та VBLAST відомі як матриці A і B, відповідно, та застосовуються залежно від статистичних параметрів каналу (відношення сигнал/шум (Signal-to-Noise Ratio, SNR), рівень кореляції у каналі, доплерівський зсув частот та інше).

Слід зазначити, що технологія багатoeлементних антен MIMO використовується не тільки для цивільних потреб. У збройних силах (ЗС) провідних країн світу вже заявлено про використання радіостанцій, що підтримують технологію MIMO. На жаль, на сьогодні перелік таких радіостанцій невеликий: Falcon III RF-7800W (корпорація L3Harris), Aselsan GRC-5220 (корпорація Aselsan), Streamcaster 4200 Enhanced Plus та 4400 Enhanced, Hydra (компанія Silvus Technologies). На озброєнні ЗС України також є засіб військового радіозв'язку вітчизняного виробництва з підтримкою MIMO 2×2 за протоколом IEEE 802.11n: станція радіорелейна широкосмугова (СРШ-5000) Р-402 виробництва компанії Telecard.

На основі аналізу модуляційно-кодових схем MCS (Modulation and Coding Scheme) станції Р-402 визначено: MCS 8 – 15 з MIMO 2×2 (Додаток А Посібника з експлуатації) застосовуються лише у варіантах виконання Р-402.02, Р-402.03 та Р-402.04, при цьому мультиплексується два незалежних просторових інформаційних потоки за способом SMX.

Проведені дослідження показують, що у найменшій MIMO 2×2 просторове рознесення сигналів за схемою Аламоуті виявляється енергетично ефективнішим порівняно з просторовим мультиплексуванням (коди типу VBLAST) при показниках СЕ до 8 біт/с/Гц. Забезпечуючи достатньо високу достовірність передачі інформації (ймовірність бітової помилки $P_{\text{п}} = 10^{-5}$) OSTBC Аламоуті дає енергетичний виграш (ЕВ) порівняно з NOSTBC VBLAST близько 2 – 10 дБ залежно від показника СЕ. Такий результат пояснюється недостатнім порядком рознесення сигналів у схемах типу VBLAST, що не перевищує кількості приймальних антен. У схемі Аламоуті порядок рознесення сигналів дорівнює подвоєній кількості приймальних антен, а тому при невеликих розмірах M ансамблю сигналів фазової (Phase Shift Keying, M-PSK) або квадратурно-амплітудної (Quadrature Amplitude Modulation, M-QAM) модуляції ($M \leq 256$) просторове рознесення сигналів є практично безальтернативним.

У MIMO 4×4 пріоритетність застосування OSTBC та NOSTBC кардинально протилежна, оскільки ортогональні породжувальні матриці OSTBC неспроможні забезпечити високі показники СЕ через відсутність виграшу мультиплексування. Застосування кодів OSTBC є економічно виправданим та енергоефективним рішенням виключно у системах MISO, коли базова станція комплектується багатоантенним передавачем, а одноантенні мобільні термінали зберігають компактність та прийнятну складність алгоритмічної та технічної реалізації.

З урахуванням отриманих результатів, рекомендовано замінити у модуляційно-кодових схемах MCS 8 – 13 станції радіорелейної широкосмугової (СРШ-5000) Р-402 спосіб просторового мультиплексування сигналів типу VBLAST на спосіб просторового рознесення сигналів за схемою Аламоуті без зміни типів модуляції, кодування та смуги частот. Отриманий ЕВ (близько 2 – 10 дБ при $P_{\text{п}} = 10^{-5}$, залежно від необхідної СЕ) забезпечить одну з таких можливостей (або їх комбінацію):

- зменшення потужності передавача без втрати завадостійкості;
- підвищення рівня достовірності прийому інформації;
- зменшення вимог до чутливості приймача;
- збільшення зони покриття базової станції;
- підвищення швидкості передачі інформації.

У радіостанціях компанії Silvus Technologies передбачено адаптивне застосування способів SMX, SD та BF залежно від статистичних параметрів каналу. Оскільки динамічно-плинна завадова обстановка передбачає часту зміну рівня просторової кореляції, фазової нестаціонарності каналу та відношення сигнал/шум, у програмному забезпеченні сучасних засобів безпроводового зв'язку спеціального призначення з підтримкою MIMO слід передбачити перемикання режимів (способів) передачі цифрової інформації на основі вимірювання та контролю зазначених показників.

МАТЕМАТИЧНА МОДЕЛЬ ПРОГНОЗУВАННЯ РАДІОЗВ'ЯЗНОСТІ ВУЗЛІВ В РАДІОМЕРЕЖАХ КЛАСУ MANET

Актуальність дослідження. Функціонування мобільних радіомереж (МР) класу MANET в умовах частоті зміни обстановки (оперативної, тактичної, зі зв'язку, тощо) передбачає зміну топології радіомережі. Приймаючи до уваги те, що зв'язок між вузлами МР може бути забезпечений лише за умов наявності радіозв'язності між ними, питання прогнозування радіозв'язності за умов високої динаміки зміни топології МР є актуальним. Окрім того, забезпечення ефективного управління МР, а також здатності їх вузлів до самоорганізації та адаптації до різних умов функціонування, можливе лише за наявності вузлової системи управління, здатної приймати управляючі рішення за умов невизначеності. Враховуючи зазначене, в ході дослідження запропоновано інтелектуалізувати процеси управління радіозв'язністю вузлів МР шляхом використання технологій обробки знань.

Метою є розробка математичної моделі прогнозування радіозв'язності вузлів тактичних радіомереж класу MANET, яка забезпечить підвищення ефективності процесу передачі даних між вузлами МР.

Виклад основного матеріалу. Суть моделі полягає в інтерпретації процесу прогнозування радіозв'язності вузлів тактичних радіомереж класу MANET, за умов стохастичної невизначеності їх функціонування, за допомогою нечіткого часового ряду.

На відміну від існуючих моделей, в яких прогнозування відбувається на основі параметрів однакової фізичної природи, із залученням експертів для здійснення прогнозу та використанням навчальної вибірки великого обсягу, запропонована модель передбачає представлення радіозв'язності між вузлами мережі у вигляді нечіткого часового ряду та забезпечує прогнозування радіозв'язності між вузлами МР шляхом формування бази нечітких правил прогнозування.

Використання моделі дозволить описати радіозв'язність між вузлами мережі на підставі множини параметрів за період часу, які є різними за одиницями виміру та фізичною природою, визначити чинники, які впливають на радіозв'язність між вузлами мережі, провести короткострокове прогнозування радіозв'язності між вузлами мережі для скорочення енергетичних та часових витрат на їх передачу.

Основними перевагами запропонованої моделі є:

- використання комплексного показника оцінки стану радіозв'язності, що враховує більшість відомих параметрів оцінки;
- однозначність отриманої оцінки стану радіозв'язності;
- відносна простота математичних розрахунків;
- можливість адаптації до сигнальної обстановки в мережі;
- можливість синтезу маршруту передачі інформації, який забезпечить передачу інформації із заданою якістю;
- можливість проводити прогнозування радіозв'язності вузлів на маршруті передачі.

Висновки. Проведено аналіз математичного апарату прогнозування радіозв'язності вузлів тактичних радіомереж класу MANET. За результатами проведеного аналізу встановлено, що найбільш доцільним для прогнозування радіозв'язності є використання апарату штучних нейронних мереж, нечіткої логіки та часових рядів.

Проведено розробку математичної моделі прогнозування радіозв'язності вузлів тактичних радіомереж класу MANET. Зазначена модель може бути використана при проектуванні радіостанцій з програмованою архітектурою, зокрема, при розробці програмного забезпечення для модулів (блоків) оцінки перспективних засобів радіозв'язку, що засновані на інтерфейсах відкритої архітектури версії SCA 2.2 та призначені для функціонування в умовах активного радіоелектронного подавлення.

ПІДСИСТЕМА АВТОМАТИЗАЦІЇ РОБОТИ КУРАТОРА НАВЧАЛЬНОЇ ГРУПИ ВВНЗ НА ОСНОВІ МОБІЛЬНОГО ДОДАТКУ

Актуальність дослідження обумовлена необхідністю спростити взаємодію куратора навчальної групи з даним підрозділом.

Витрати часу пов'язані з організацією взаємодії куратора з підрозділом є фактором який зменшує ефективність роботи та навчання. Звідси випливає, що порівняв узгодження рішення задач автоматизації планування є важливим питанням, яке визначає ефективність взаємодії між ними.

Мета дослідження полягає у підвищенні ефективності процесів організації за рахунок виконання **наступних часткових завдань дослідження**:

- аналіз сучасного підходу у плануванні навчально-виховної роботи, спираючись на вимоги керівних документів;
- Дослідження існуючих рішень спрямованих на автоматизацію навчального процесу і взаємодії між керівником і підлеглими;
- розробка підсистеми спрямованої на автоматизацію взаємодії куратора та навчальної групи.

Виклад основного матеріалу. Автоматизація взаємодії між куратором та підрозділом є важливою функцією контролю за навчальним процесом, яка представляє собою процес постановки завдань, контролю за успішністю і виконання безпосередніх завдань куратора навчальної групи. Змістом процесу планування є розподіл завдань та часу куратора, автоматизації роботи куратора з навчальною групою та визначення порядку їх взаємодії для досягнення поставлених цілей.

Одне з основних завдань при створенні підсистеми автоматизації роботи куратора є проектування її структури, яка дозволяє розподілити задачі максимально ефективно та наглядно відобразити проблеми в навчальній групі на які слід звернути увагу. Визначити максимально зручний інтерфейс та максимально повно охопити задачі вирішення яких стоїть перед куратором навчальної групи. Рішення даного завдання являє собою складний трудомісткий процес, адже необхідно максимально широко охопити всі аспекти діяльності куратора та врахувати всі задачі, які він має виконувати. Облік динаміки функціонування підсистеми на етапі її проектування призводить до необхідності спільного використання оптимізаційних та імітаційних моделей для отримання оптимальних (раціональних) варіантів побудови цієї підсистеми. В даній роботі для вирішення завдання автоматизації роботи куратора з навчальною групою запропоновано використання мобільного додатку який дозволить взаємодіяти з кожним курсантом навчальної групи та максимально повно відображати його успішність. В даній роботі для вирішення завдання автоматизації роботи куратора навчальної групи запропоновано використання "MVP-архітектуру".

Базуючись на етапи проектування структури системи, використовуючи класичний підхід проектування було розроблено узагальнену архітектуру і алгоритми роботи підсистеми. Проведено оптимізацію додатку та його тестування.

Висновки. Отже, в роботі запропоновано використання мобільного додатку для автоматизації роботи куратора з навчальною групою і на його основі реалізовано підсистему контролю успішності і постановки завдань.

ОСОБЛИВОСТІ ЗАВАДОСТІЙКОГО КОДУВАННЯ ПРИ ПЕРЕХОДІ ЧЕРЕЗ ЙМОВІРНІСНУ МЕЖУ $P \geq 10^{-2}$

Актуальність. Оцінюються особливості використання завадостійкого кодування з огляду на граничні можливості, які представлені теоремами К. Шеннона, але стосовно реальних якісних показників ліній зв'язку. Аналізується стан радіоліній щодо обміну інформацією у межах ймовірностей помилок $p = 10^{-2} \dots 10^{-1}$ на одиничний елемент, що можливо при радіоелектронному подавленні (РЕП), враховуючи технічні досягнення провідних держав світу у створенні відповідних систем радіоелектронної боротьби. Представлене значення $p = 10^{-2}$ було граничним при розробці апаратури передачі даних попередніх етапів розвитку систем зв'язку на теренах СНД, і воно залишається актуальним для сучасних розробок, особливо при $p > 10^{-2}$, якщо не ігнорувати і прийняти до уваги такий можливий стан радіоліній. Заграницні стандарти не орієнтують розробників апаратури на $p = 10^{-2}$ – і в цьому небезпека, тому що використання такої апаратури при суттєво погіршених умовах зв'язку може привести до втрати зв'язку.

Аналіз задачі. Лінії (і відповідно канали) зв'язку характеризуються різним якісним станом, що суттєво впливає на показники вірогідності (вірності) обміну повідомленнями. На інформаційний сигнал діють різні спотворювальні фактори (шуми), які залежать від типу лінії, діапазону частот, зовнішніх та внутрішніх електромагнітних впливів, методів передачі та обробки сигналів. У таких умовах забезпечення практично прийнятної для конкретних потреб ідентичності переданих і прийнятих повідомлень є важливою технічною задачею. Відповідно й формуються методи підвищення вірогідності стосовно задач обміну інформацією з використанням конкретних телекомунікаційних систем, зокрема, військового призначення. Практика показала, що розв'язання якимось одним способом неможливе, необхідне використання сукупності різних методів. Узагальнюючих методів оптимізації, які б визначали сполучення найбільш раціональних методів, стосовно отримання найкращого очікуваного ефекту для даних умов, нема, а існують лише часткові оптимізаційні рішення, порівняльні оціночні дані та граничні орієнтири.

На різних лініях зв'язку ймовірність помилкового прийому одиничного елементу (1 та 0) може складати в середньому $p \approx 10^{-2} \dots 10^{-5}$, на волоконно-оптичних – менше. В умовах РЕП на радіолініях можливе збільшення p до значення $p \approx 10^{-2} \dots 10^{-1}$. Потреби у забезпеченні ймовірності помилок на інформаційний знак $P_{\text{зн}}$ на виході приймального тракту апаратури можуть коливатися в межах $P_{\text{зн}} = 10^{-6} \dots 10^{-10}$ у залежності від цільового використання телекомунікаційних систем. Тому різні засоби зв'язку характеризуються у певній мірі власними варіантами використання методів підвищення вірогідності і дослідження в цій області продовжуються. Практика розробок та експлуатації ряду різних за призначенням телекомунікаційних систем показала значну частку їх ідентичності в показниках і характеристиках, що створило підґрунтя для стандартизації сукупності параметрів]. Межа $p = 10^{-2}$ встановлювалась при розробці спеціальних систем передавання даних у спеціалізованих державних структурах до утворення СНД, а потім і на терені СНД. Величина $p = 10^{-2}$ значно жорсткіша, ніж це прийнято нормами МСЕ-Т. Зокрема, у цифровому потоці $E1$ ймовірність помилок допускалась міжнародними стандартами не більше $p = 10^{-4}$, пізніше це значення було МСЕ-Т скореговане до величини $p = 10^{-3}$. Якщо реальні значення p на лініях зв'язку перевищують цю норму, то апаратура переходить в аварійний режим із від'єднанням від абонентів усіх каналів, що неприйнятно для польових систем військового зв'язку.

В Україні діють європейські стандарти щодо потоків $E1$, $E2$ тощо. Тому безпосереднє використання відповідної закордонної апаратури в системі спеціального зв'язку

проблематичне із-за необхідності збільшення параметра p до величини $p = 10^{-2}$. Крім цього, потрібна додаткова модернізація апаратури щодо польових умов її використання, які жорсткіші від комерційних стандартів. Розв'язання цих питань стосовно систем, що формують потоки $E1$, $E2$, які найбільш доцільні для використання, виходячи із структур ланок управління, можливе на основі застосування різних методів підвищення вірогідності, відповідної елементної бази та технологічних рішень.

Необхідність аналізу методів підвищення вірогідності обміну повідомленнями при ймовірностях $p > 10^{-2}$, зокрема, у межах $p = 10^{-2} \dots 10^{-1}$, зумовлена можливостями сучасних засобів радіоелектронної боротьби (РЕБ) щодо створення суттєво непростих умов функціонування всіх видів радіозв'язку, що підтверджує досвід локальних і регіональних війн. При переході ймовірностей через значення $p > 10^{-2}$ ряд алгоритмів підвищення вірогідності втрачають ефективність, зокрема, завадостійке кодування. Так, при зростанні ймовірностей помилок до величини $p = 10^{-2}$ у кодовій комбінації завадостійкого коду, довжиною, наприклад, $n = 70 - 150$ елементів, можуть виникнути 1 – 3 помилки, які код здатний виправити. При збільшенні p до значення $p = 10^{-1}$ у цих кодових комбінаціях буде 7 – 15 помилок, виправлення яких уже проблематичне, тому можуть використовуватись варіанти повторення кодових комбінацій для зменшення в них ймовірностей помилок перед декодуванням. Стає очевидною недоцільність використання кодових комбінацій великої довжини. Повторення та зменшення довжини n до кількох десятків знижує інформаційну ефективність використання каналів і ліній зв'язку, що не відповідає сучасним тенденціям завадостійкого кодування, зокрема, у моделах для роботи по каналах ТЧ передбачена протоколами V.34, V.90, V.92 довжина кодових комбінацій в сотні і тисячі елементів. Але у спеціалізованих системах може виникнути критична ситуація, коли потрібно забезпечити передачу хоч би якимось чином, з огляду на надзвичайну важливість інформації і її значення для управління бойовими діями, тому використання нестандартизованих алгоритмів функціонування систем стає необхідним.

Найбільш “важкими” стосовно підвищення вірогідності є радіосистеми, особливо спеціалізованого та військового характеру, які з високою ймовірністю можуть подавлятися радіозасобами протидіючої сторони, до речі, достатньо ефективними, що вимагає об'єктивного критичного їх оцінювання. Треба зазначити, що при виникненні та розв'язуванні завдань управління (нерідко, суттєво екстрених), пов'язаних також з переміщеннями військових об'єктів, змінами топологічних даних, можливими втратами, забезпечення зв'язку, навіть з погіршеними характеристиками, є особливо важливим. Тому, як правило, проектування відповідних систем велося (і це питання залишається актуальним) із орієнтацією на найгірші умови функціонування. Такій апаратурі властиві надмірності, часто суттєві, у структурній побудові та функціональних рішеннях, зокрема, стосовно методів підвищення вірогідності, але це себе оправдовувало, з огляду на важливість задач, які розв'язувались, навіть при високих економічних затратах. Такі питання є актуальними взагалі, але особливу вагу вони мають для тактичної ланки, яка безпосередньо стикається з ворогом, і управління життєво необхідне при будь-яких варіантах розвитку ситуацій.

В умовах РЕП пряме використання завадостійкого кодування (без додаткових операцій над інформаційними елементами) може виявитись неефективним із-за нездатності коду виправляти і виявляти помилки великої кратності. Певним “облегшенням” функціонування коду може бути перемішування інформаційних елементів перед кодуванням, що веде до декореляції пакетів помилок у прийнятій інформаційній послідовності і покращує у певній мірі результати декодування. Можливість зменшення впливу РЕП дає зміна частот обміну по псевдовипадковому алгоритму (ППРЧ), кілька кратно повторення повідомлення у часі, на різних частотах, а також з використанням антено-просторових алгоритмів (типу МІМО). У системах із повтореннями доцільною є обробка прийнятих копій сигналу перед демодуляцією, з метою підвищення відношення сигнал/шум, що дає додаткове зменшення ймовірностей помилок у кожній кодовій комбінації перед застосуванням алгоритму формування вихідних рішень щодо повідомлення в цілому на основі множини прийнятих і

декодованих комбінацій. Треба відмітити, що для таких умов повинні бути вибрані певні довжини як повідомлення, так й інформаційних кодових комбінацій.

Для розв'язання задач підвищення вірогідності прийому використовують ті методи, які найкраще підходять для умов застосування апаратури, наприклад, у цифрових системах передачі мови є обмеження на затримку сигналу, тому зворотний зв'язок може бути малоефективним, веде до ненатуральності мовного процесу, аналогічно, зворотний зв'язок проблематичний у дальньому космічному зв'язку, коли розповсюдження сигналу триває хвилинами, або у системах, в яких використовується режим радіомовчання. У системах CDMA є жорсткі обмеження на потужність передавача, тому підвищити відношення потужностей сигнал/шум за рахунок передавача недоцільно. У системах радіолокації жорсткий час на обробку інформації обмежує варіанти зворотного зв'язку, який вносить певний елемент випадковості із-за невизначеної кількості запитів по зворотному каналу і, відповідно, повторень.

Треба зазначити, що у деяких спеціалізованих системах є доцільним кількаразове повторення повідомлення, як додатковий режим роботи, якщо знехтувати зниженням інформаційної ефективності використання каналу зв'язку, зате можна отримати можливість підвищення вірогідності. У комерційних системах кількаразове зниження інформаційної ефективності каналу економічно нераціональне, тому такі методи можуть використовуватись у тих системах, в яких пріоритетною задачею є підвищення вірогідності.

Повторення повідомлень (кодових комбінацій) може бути орієнтоване на той варіант обробки прийнятих сигналів, який забезпечує краще відношення сигнал/шум при демодуляції, чи на зменшення перед декодуванням ймовірностей помилок у результатній кодовій комбінації, утвореної з прийнятих копій комбінацій. Останній варіант відповідає **мажоритарному** способу прийняття рішення за правилом більшості щодо однойменних розрядів цих копій при формуванні відповідних розрядів результатної кодової комбінації.

Повторення може бути реалізоване програмно у вигляді переходу від стандартизованого алгоритму обміну (без повторень) до обміну з повтореннями при погіршенні якості ліній зв'язку. Такий перехід хоча і знижує інформаційну ефективність каналу зв'язку, але він доцільний, як додатковий режим функціонування в системах, в яких вимоги щодо забезпечення вірогідності обміну превалюють над інформаційною ефективністю використання каналу зв'язку.

Мажоритарний принцип передбачає непарне число повторень і може бути реалізованим послідовною передачею по каналу, одночасною передачею по паралельних каналах, дублюванням сигналу по кількох частотних каналах або у вигляді просторового алгоритму обробки електромагнітних коливань за принципом МІМО. Доцільним є трикратне повторення, при якому інформаційна ефективність використання каналу зв'язку зменшується мінімальне число раз (майже у три рази). Зростання кількості повторень (5; 7) зменшує кількість помилок у результатній кодовій комбінації, але ще більше знижує інформаційну ефективність каналу зв'язку, тому доцільність таких повторень потребує обґрунтувань.

Висновки

1. Представлений аналіз необхідності використання методів підвищення вірогідності обміну повідомленнями та ефективності завадостійкого кодування в умовах ймовірностей помилок на радіолініях у межах $p = 10^{-2}$ та більше, що відповідає умовам РЕП.

2. Показано, що довгі коди в таких умовах неефективні, а використання коротких потребує суттєвих ускладнень, тому доцільними є принципи повторення кодових комбінацій, що облегшує процес декодування, хоча знижує інформаційну ефективність використання каналу зв'язку.

3. Розглянуті особливості використання принципу мажоритарного опрацювання прийнятих копій кодових комбінацій завадостійкого коду для підвищення ефективності декодування і підвищення вірогідності обміну.

АУДИТ СТАНУ КІБЕРЗАХИСТУ, ЯК СКЛADOVA ОЦІНКИ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ З УРАХУВАННЯМ ІНДИКАТОРІВ КІБЕРЗАГРОЗ

Оцінка стану кіберзахисту об'єктів критичної інформаційної інфраструктури будь якого масштабу є об'єднанням та пошуком кореляції між даними аудиту стану кіберзахисту об'єктів критичної інфраструктури, даними щодо оцінки ризиків та моделей кіберзагроз, даними про індикатори, що передують відомим кіберзагрозам, даними моделювання впливу кіберзагрози на об'єкти критичної інфраструктури за декількома, найбільш ймовірними, сценаріями. Також слід враховувати, що кібератаки мають різні фази, частоту повторень, періоди та види, тому проведення аудиту поточного стану кіберзахисту об'єктів критичної інфраструктури певним індикаторам є невід'ємною та первинною складовою оцінки стану кіберзахисту критичної інформаційної інфраструктури. Аудит стану кіберзахисту об'єктів критичної інфраструктури – це комплексна перевірка стану кібербезпеки організації, що забезпечує функціонування критичної інформаційної інфраструктури, яка включає в себе: аудит бізнес-процесів організаційної структури; аудит нормативного забезпечення; аудит ІТ інфраструктури організації, що експлуатує та відповідає за критичну інформаційну інфраструктуру; аудит процесів кібербезпеки; оцінку технічної захищеності (сканування і тестування на проникнення); оцінку стійкості компанії до соціальної інженерії; аудит інформаційних потоків в організації; аудит безпеки процесів аутсорсингу.

Технічна складова аудиту стану кіберзахисту ширша, ніж просто інвентаризація програмних і апаратних засобів безпеки з вибіркоким переглядом налаштувань. Це, в першу чергу, перевірка дотримання стандартів та політик (протоколів) інформаційної безпеки, а також зовнішнє і внутрішнє тестування на проникнення для визначення вразливостей, в тому числі, з використанням соціальної інженерії, перевірки відповідності навиків та якостей співробітників в середині організації, що можуть вплинути на стан інформаційної безпеки. Аудит стану кібербезпеки може бути як пасивним так і активним.

Результатами якісного аудиту стану кіберзахисту є: висновки аудиту інформаційної безпеки в установах, організаціях, де використовуються об'єкти критичної інформаційної інфраструктури, та виявлені порушення затверджених законодавством вимог захисту інформації; висновки аудит стану спроможності кіберзахисту ІТ інфраструктури об'єкту критичної інформаційної інфраструктури щодо виявлення, попередження інцидентів кібербезпеки, відповідно до стандартів (ISO 2700x, NIST, AICPA, HITRUST, COBIT, PCI DSS, GDPR, SOX, SWIFT, HIPPA, NYDFS); інформація про стан організацій, пов'язаних інформаційними потоками з об'єктом критичної інформаційної інфраструктури, установ, інших держав та стан організації кіберзахисту інформаційного обміну між ними; розрахункові показники можливості відновлення функціонування після кібератаки та наявність нормативного забезпечення порядку відновлення; відповідність результатів аудиту моделі ризиків та загроз, яка була визначена для даного об'єкту критичної інформаційної інфраструктури.

Отже, застосування нормативно регламентованого аудиту стану кіберзахисту до об'єктів, які експлуатують критичну інформаційну інфраструктуру, дозволить обґрунтовувати перелік змін в моделях ризиків та загроз зазначених об'єктів, використовувати дані аудиту для здійснення моделювання та прогнозування наслідків кібератак у загальнодержавному центрі кіберстійкості CRC (*Cyber Resilience Center*). Подальшим напрямком досліджень є дослідження різних типів даних, які можуть бути отримані з диференційованих джерел інформації та програмних платформ, що здатні здійснювати обробку великих даних, і можуть використовуватись для оцінки стану кіберзахисту об'єктів критичної інформаційної інфраструктури в режимі реального часу, з урахуванням індикаторів кіберзагроз.

МОДЕЛЬ ПЕРЕДАЧІ ІНФОРМАЦІЇ В МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ НА ОСНОВІ ПРОТОКОЛУ QUIC

Актуальність дослідження. На сучасному етапі розвитку Збройних Сил України, одним з провідних напрямків є впровадження нових ідей для покращення передачі інформації в мережах спеціального призначення. Новітні протоколи для передачі даних в першу чергу призначені для покращення процесу управління на всіх ланках управління.

Метою дослідження є модель передачі інформації в мережах спеціального призначення за допомогою впровадження протоколу QUIC.

Виклад основного матеріалу.

На сьогоднішній день всі ІТ-компанії працюють над проектами щодо зменшення затримки передачі пакетів між вузлами та серверами. Найпоширенішим протоколом в світі є TCP/IP, проте, в порівнянні з протоколом QUIC він має певні недоліки по всім параметрам (RTT– затримки, середнє арифметичне затримок, втрати пакетів тощо). **QUIC** (англ. Quick UDP Internet Connections) – транспортний мережевий протокол, який впроваджується компанією Google з 2013 року як альтернатива зв'язці TCP + TLS для web. Він вирішує проблеми з часом встановлення і узгодження з'єднань в TCP і усуває затримки при втраті пакетів в процесі передачі даних. QUIC є надбудовою над протоколом UDP, що підтримує мультиплексування декількох з'єднань і забезпечує методи шифрування, еквівалентні TLS/SSL. Протокол вже інтегрований в серверну інфраструктуру Google, входить до складу Google Chrome, запланований для включення в Firefox і активно застосовується для обслуговування запитів клієнтів на серверах Google. Протокол HTTP/3 реалізує надбудову для забезпечення роботи HTTP поверх протоколу QUIC, як показано на рисунку нижче.

Протокол QUIC має наступні переваги, нижче приведені деякі з них:

- Високий рівень безпеки, аналогічний TLS;
- Контроль за цілісністю потоку, що запобігає втраті пакетів;
- Можливість миттєво встановити з'єднання;
- Межі криптографічних блоків вирівняні з межами пакетів QUIC, що зменшує вплив втрат пакетів на декодування вмісту наступних пакетів;
- Відсутність проблем з блокуванням черги TCP.

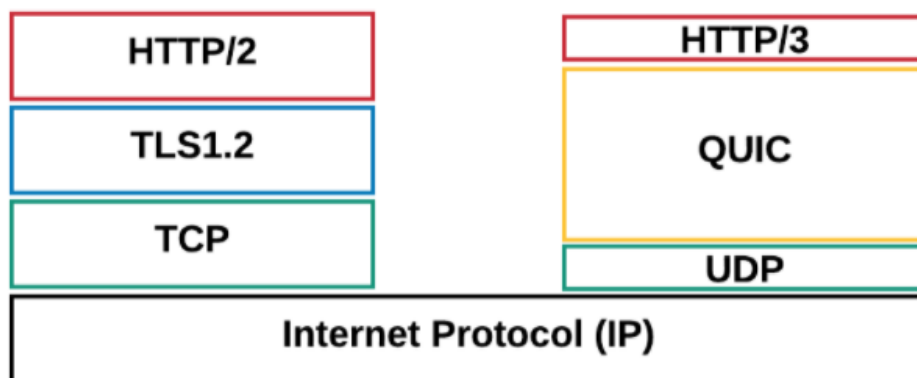


Рис. 1 Представлення QUIC

Висновки. Застосування протоколу QUIC дозволить замінити в майбутньому протокол TCP: установка з'єднання, подолання HoL-блокування, керування перенавантаженнями, міграція з'єднання. З даним протоколом можна покращити полегшити передачу інформації незалежно від мережі та регіону, зробивши зручний та безшовний транспорт пакетів більш доступним по всьому світу.

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ ПРОЦЕСУ ПЕРЕДАЧІ ПОВІДОМЛЕНЬ У КАНАЛАХ ЗВ'ЯЗКУ З ВИСОКОШВИДКІСНИМИ ОБ'ЄКТАМИ ЗА УМОВ НЕЛІНІЙНОГО ДОППЛЕРІВСЬКОГО ЗСУВУ ЧАСТОТИ

Актуальність дослідження. Для максимальної реалізації можливостей методу неортогональної частотної дискретної модуляції сигналів (N-OFDM) при забезпеченні зв'язку з мобільними абонентами важливу роль відіграє врахування потенційно-досяжної точності оцінювання величини доплерівських зсувів частот піднесучих. Це необхідно для правильного вибору порядку квадратурно-амплітудної модуляції, використовуваної при передачі інформації, і адаптивної його зміни. Суть моделювання зводилася до імітації процесу передачі повідомлень по каналу зв'язку з високошвидкісним об'єктом на основі обробки сигналів відповідно до запропонованих методів компенсації ефекту Доплера та нелінійної частотної модуляції [1, 2]. **Метою моделювання** являвся доказ можливості достовірної передачі даних і їх правильної демодуляції в умовах нелінійного доплерівського зсуву частоти, а також перевірка справедливості отриманих аналітичних співвідношень для нижніх границь Крамера-Рао моделі оцінювання дисперсій помилок демодуляції OFDM сигналів при зв'язку з високошвидкісними об'єктами [3].

У якості моделі сигналу було прийнято його комплексне представлення по виходах прийомних каналів лінійної ЦАР відповідно до виразів для квадратурних складових напруг виду:

$$U_{s,r}^c = \sum_{m=1}^M (a_m^c \cos p_{msr} - a_m^s \sin p_{msr}) + n_{s,r}^c; U_{s,r}^s = \sum_{m=1}^M (a_m^c \sin p_{msr} + a_m^s \cos p_{msr}) + n_{s,r}^s, \quad (1)$$

де $a_m^c = a_m \cdot \cos \varphi_m$, $a_m^s = a_m \cdot \sin \varphi_m$,

$$p_{smr} = \frac{2\pi d}{\lambda} r \cdot \sin \theta + \omega_m \Delta t (s-1) - \omega_{0m} R_s / c; R_s = \sqrt{R_0^2 - 2VR_0(s-1)\Delta t \cos \varepsilon + V^2 \Delta t^2 (s-1)^2},$$

M – порядковий номер піднесучої,

r – порядковий номер прийомного каналу ЦАР,

d – інтервал між фазовими центрами антенних елементів ЦАР (крок ґрат),

θ – азимутальний напрямок на високошвидкісний об'єкт (покладається незмінним протягом сигнальної вибірки),

$n_{s,r}^c, n_{s,r}^s$ – квадратурні складові напруг шумів.

Для генерації шумів використовувався датчик некорельованих випадкових чисел, розподілених за нормальним законом із заданою дисперсією і нульовим математичним очікуванням. Набір статистики здійснювався по 100 реалізаціях. Перевірка справедливості НГКР здійснювалася з урахуванням довірчого інтервалу, розрахованого для довірчої ймовірності 0,95. Найпростіша з розроблених і досліджених математичних моделей забезпечувала імітацію одночасного прийому одночастотних сигналів від двох ($G = 2$) високошвидкісних БПЛА, з довільним кутовим рознесенням по азимуту. При цьому передбачалося, що швидкості польоту V , початкові відстані від приймального пункту R_0 , кути місця ε і їх еволюція в часі для обох БПЛА однакові. У зазначеному випадку аналітичні співвідношення для напруг сигналів по виходах лінійної ЦАР мають вигляд:

$$U_{s,r}^c = \sum_{g=1}^2 a_g^c \cos p_{gsr} - a_g^s \sin p_{gsr} + n_{s,r}^c; U_{s,r}^s = \sum_{g=1}^2 a_g^c \sin p_{gsr} + a_g^s \cos p_{gsr} + n_{s,r}^s, \quad (2)$$

$$\text{де } p_{gsr} = \frac{2\pi d}{\lambda} r \cdot \sin \theta_g + \omega_g \Delta t (s-1) - \omega_g R_s / c, R_s = \sqrt{R_0^2 - 2VR_0(s-1)\Delta t \cdot \cos \varepsilon + V^2 \Delta t^2 (s-1)^2}.$$

У процесі моделювання зміні підлягали кількість антенних елементів лінійної ЦАР, тривалість оброблюваної часової вибірки напруг сигналів, значення частот піднесучих, просторове рознесення по азимуту і параметри руху БПЛА.

Амплітуди сигналів задавалися в квантах АЦП, азимути джерел сигналів – в узагальнених кутових координатах, відлік яких ведеться щодо нормалі до ЦАР і виражених в частках ширини $\Delta\theta$ головного променя діаграми спрямованості приймальної ЦАР, синтезованої за допомогою операції швидкого перетворення Фур'є. Аналогічно, частоти піднесучих встановлювалися в значеннях узагальненої частоти, вираженої у частках величини $\Delta F = (S \cdot \Delta t)^{-1}$, де S – кількість відліків АЦП в оброблюваній вибірці, Δt – період дискретизації АЦП. В ході досліджень було підтверджено працездатність запропонованих методів демодуляції сигналів, для чого кожна з піднесучих використовувалася для передачі двохсимвольних повідомлень, наприклад, виду „FB” і „rl” які в подальшому відновлювалися по виходу блоку алгоритмів обробки прийнятих сигналів.

Для зручності декодування символів ASCII вся апертура АЦП розбивалася на 255 символних інтервалів. Величина міжсимвольного інтервалу задавалася з урахуванням розрядності АЦП, порядку квадратурного-амплітудної модуляції (QAM) і необхідної ймовірності правильної передачі повідомлень. Еквівалентом відносини сигнал-шум в розглянутих моделях стало відношення величини міжсимвольного інтервалу до середньоквадратичного відхилення (СКВ) оцінок амплітуд.

На рис. 1 наведено графік, що ілюструє залежність СКВ оцінок квадратурних складових амплітуд сигналів від кількості елементів в ЦАР, отриману для випадку $V=1000$ м/с, висоти польоту БПЛА 5000 м і горизонтальної початкової дальності до них – 5000 м, азимутальних координат БПЛА 0 і $0,5\Delta\theta$, частот піднесучих сигналів 0 і $0,001\Delta F$. При цьому вплив кількості антенних елементів на величину СКВ досліджувався для фіксованих часових вибірок.

Уздовж горизонтальної осі відкладено кількість антенних елементів (R) в ЦАР. По-вертикалі наведені СКВ оцінок чотирьох квадратурних складових амплітуд двох гармонійних сигналів в квантах АЦП. Пунктирною лінією показана НГКР, перерахована для СКВ. Сімейство кривих, отриманих в результаті моделювання, облямоване на графіках межами довірчого інтервалу: трикутним маркером відзначена його верхня межа, прямокутним – нижня.

Висновки. Результати моделювання дозволили переконаватися в справедливості гіпотези про те, що СКВ помилок оцінювання амплітуд сигналів знижується зі збільшенням кількості антенних елементів R в решітці і тривалості сигнальної вибірки S пропорційно і відповідно. Свідченням достовірності отриманих аналітичних виразів для НГКР є потрапляння всіх експериментальних залежностей в межі довірчого інтервалу.

ЛІТЕРАТУРА

1. Патент України на корисну модель № 46668. Спосіб випереджувальної компенсації ефекту Доплера при передачі OFDM сигналів. (патент)
2. Слюсар В.І., Троцько О.О. Нелінійна частотна модуляція OFDM сигналів при зв'язку з високошвидкісними літальними апаратами. Сучасні інформаційні технології у сфері безпеки та оборони. 2015. № 1 (22).– С. 118 – 124.
3. Слюсар В.І., Остапчук В.М., Симоненко О.А., Троцько О.О. Модель оцінювання дисперсій помилок демодуляції OFDM сигналів при зв'язку з високошвидкісними об'єктами. Збірник наукових праць ВІПІ. - № 1. – 2019. – с. 91 – 96.

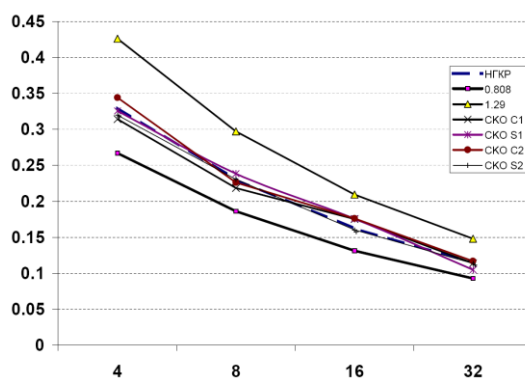


Рис. 1. Залежність СКВ оцінок квадратурних складових амплітуд сигналів від кількості елементів в ЦАР при 4-відлікової тимчасової вибірки.

МОДЕЛЮВАННЯ ПРОЦЕДУРИ ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ВІД КІБЕРАТАК

Проблеми забезпечення інформаційної безпеки у воєнній сфері, з огляду на появу нових та зростання рівня існуючих ризиків і загроз в інформаційному просторі України, набувають великої значущості і потребують відповідного наукового підґрунтя для їх вирішення. Є низка публікацій, що присвячені проблемам інформаційної безпеки в інформаційних системах і мережах передачі та обробки інформації. Завдання створення, організації і дослідження процесів функціонування, удосконалення й розвитку систем забезпечення безпеки інформації тою чи іншою мірою висвітлені в працях. Однак дотепер повною мірою не вивчені та залишаються дискусійними методологічні, методичні й практичні аспекти дослідження проблем моделювання безпеки складних інформаційних систем. При цьому не існує загальноприйнятих стандартів або підходів, що дозволяють забезпечити підвищений або високий рівень захисту. Пошук методичних, практичних, аспектів дослідження проблем моделювання захищеності інформаційно-телекомунікаційних систем. **Мета.** Викладення методу комплексного оцінювання рівня безпеки інформаційних систем, що ґрунтується на якісних шкалах і відношенні переваги між факторами в структурі ієрархії цих факторів. **Основні положення.** Під рівнем інформаційної безпеки системи розуміється оцінка, яка отримана із сукупності показників і критеріїв, що характеризують стан системи на предмет захищеності критичних для неї елементів. Рівень інформаційної безпеки системи можна характеризувати за такою матрицею:

$$B = \begin{pmatrix} K1 & F1 & V1(T) & S1 \\ K2 & F2 & V2(T) & S2 \\ \cdot & \cdot & \cdot & \cdot \\ Kn & Fn & Vn(T) & Sn \end{pmatrix},$$

де K_i – показник рівня безпеки за i -м критерієм; F_i – тенденція зміни i -го критерію; $V_i(T)$ – швидкість зміни i -го критерію, що є функцією часу T ; S_i – ступінь критичності негативних наслідків при реалізації загроз, яка погіршує значення i -го критерію. Перший і четвертий стовпці являють собою вектор часткових критеріїв безпеки і їх ваги та характеризують поточний стан комплексної інформаційної безпеки, даючи змогу оцінити ситуацію, що склалася на даний момент часу. Другий і третій стовпці матриці відображають динаміку розвитку процесів та дають змогу прогнозувати їх розвиток у подальшому.

Дана матриця реалізовується за допомогою методу аналізу ієрархій (МАІ). МАІ - математичний інструмент системного підходу до складних проблем прийняття рішень. Метод дозволяє зрозумілим і раціональним чином структурувати складну проблему прийняття рішень у вигляді ієрархії, порівняти і виконати кількісну оцінку альтернативних варіантів рішення. У вершині ієрархії в МАІ розташовується основна мета, далі, на рівень нижче – підцілі, та нарешті, на самому нижньому рівні – альтернативи, серед яких проводиться вибір або ранжування. Для процесу парного зважування експертом елементів ієрархії в МАІ використовується інтуїтивно обґрунтована якісна шкала. Для визначення альтернативи підходу для забезпечення інформаційної безпеки, експерту з інформаційної безпеки необхідно враховувати досить велику кількість показників, критеріїв та неупорядкованих факторів, для того щоб оптимізувати його роботу буде використовуватись програмне забезпечення яке базується на МАІ, що призначене для підтримки прийняття зважених рішень в сферах людської діяльності “MPriority 1.0”. **Висновок.** Отже, запропонований метод моделювання процесу оцінювання інформаційної безпеки на основі експертних висновків може бути застосований для оцінювання комплексної безпеки різних систем. При цьому елементи, що характеризують систему, утворюють ієрархію, а фактори одного підрівня ієрархії полягають у відношенні переваги один до одного. Даний метод можливо реалізувати за допомогою програмного забезпечення “MPriority 1.0”.

ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Сучасні інформаційно-телекомунікаційні системи спеціального призначення є орієнтованими, в першу чергу, на обробку інформації з обмеженим доступом, яка є власністю держави. Відповідно до вимог законодавства для забезпечення конфіденційності, доступності, цілісності та спостереженості інформації в таких ІТС повинна створюватися система захисту інформації (СЗІ), як невід’ємна її складова. СЗІ являє собою складну організаційно-технічну, економічну й інформаційну систему, і, як правило, складається з організаційних та інженерних заходів, фізичних засобів захисту, комплексу технічного захисту інформації (ТЗІ) та комплексу засобів захисту від несанкціонованого доступу.

Метою технічного захисту інформації є запобігання витoku технічними каналами або порушення *цілісності інформації* з обмеженим доступом. Аналіз наукових праць та публікацій, присвячених забезпеченню ефективного захисту інформації свідчить про те, що підвищення безпеки інформації в ІТС СП можливе лише при комплексному підході до аналізу можливих загроз й удосконалення засобів захисту від них.

Загрозами будемо називати шляхи реалізації дій, які вважаються небезпечними з погляду забезпечення захищеності інформації. Таким чином, загроза – це потенційно можливий несприятливий вплив на інформацію, що призводить до порушення конфіденційності, цілісності, доступності інформації, відмови в обслуговуванні тощо.

Оцінка ефективності функціонування СЗІ можлива на підставі аналізу узагальненої моделі її взаємодії з навколишнім середовищем. Причому узагальнена модель повинна відображати процес захисту інформації як взаємодію дестабілізуючих факторів і засобів захисту.

В даний час широко використовується узагальнена ймовірнісна модель процесу захисту інформації, представлена на рис. 1. У відповідності до неї обробка інформації на об’єкті O_i

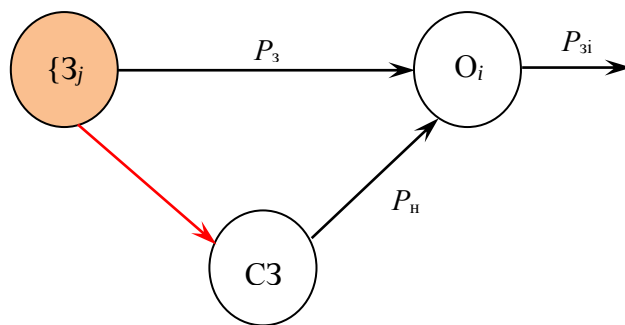


Рис. 1. Узагальнена модель процесу захисту

здійснюється в умовах впливу на інформацію різних загроз $\{Z_j\}$. Для забезпечення інформаційної безпеки об’єкту СЗІ повинна здійснювати нейтралізуючий вплив на дестабілізуючі фактори та загрози. Ймовірність ефективного захисту інформації від j -ї загрози P_{zij} можна визначити наступним чином:

$$P_{zij} = 1 - P_{zj}(1 - P_{nj}),$$

де P_{zj} – ймовірність впливу j -ї загрози на i -й об’єкт, P_{nj} – ймовірність нейтралізації впливу j -ї загрози. Тоді загальну ефективність СЗІ P_{csi} (ймовірність захисту інформації від усіх можливих загроз n) запишемо, як

$$P_{csi} = \prod_{j=1}^n P_{zij}.$$

Тому метою роботи є аналіз можливих загроз цілісності інформації в ІТС СП та визначення методів захисту від них. Цілісність забезпечується шляхом дотримання вимог політики безпеки по переміщенню інформації від відправника до отримувача. Під повнотою

захисту при обміні, варто розуміти врахування багатьох можливих типів загроз, від яких забезпечується захист.

Серед способів захисту від порушень цілісності можна виділити наступні:

- введення надмірності в саму інформацію (використання коригувальних кодів);
- введення надмірності в процес обробки інформації (використання процедури аутентифікації);
- введення системної надмірності (підвищення живучості системи).

Загрози, які спрямовані на індивідуальні повідомлення, передані в ІТС. Типовим об'єктом нападу може служити інформаційний обмін між двома користувачами системи.

Застосовують наступні основні методи підвищення енергетичної і структурної прихованості системи передачі:

робота з мінімально необхідною потужністю випромінювання, достатньою для забезпечення необхідної якості зв'язку, використання радіосистем з адаптацією за потужністю випромінювання;

використання оптимальних способів приймання сигналів і пристроїв захисту (подавлення) від навмисних завад;

використання складних шумоподібних сигналів з великою базою. Такі сигнали, на відміну від простих, мають більш високу завадостійкість і прихованість, а отже і ефективність при забезпеченні цілісності переданої інформації;

використання частотно-адаптивних ліній зв'язку.

Таким чином, проведений аналіз дозволяє зробити наступні висновки.

В інформаційно-телекомунікаційних системах спеціального призначення основними загрозами каналній цілісності інформації є перехоплення, несанкціоноване відтворення інформації, маскування, маніпуляції даними та радіоелектронне подавлення.

Для захисту від порушень цілісності інформації необхідно застосовувати введення надмірності в саму інформацію, у процес її обробки, а також введення системної надмірності.

Поряд з криптографічними методами захисту інформації як один з основних напрямків забезпечення цілісності інформації в інформаційно-телекомунікаційних системах спеціального призначення заслуговує на увагу застосування методів підвищення прихованості зв'язку. Серед цих методів особливе місце займають шумоподібні сигнали, що дозволяють одночасно підвищити достовірність і прихованість передачі інформації. Застосування в інформаційно-телекомунікаційних системах спеціального призначення шумоподібних сигналів та інших методів забезпечення прихованості передачі сигналів дозволить підвищити рівень захищеності інформації від порушень цілісності та інших загроз.

ЛІТЕРАТУРА

1. Закон України „Про захист інформації в інформаційно-телекомунікаційних системах”.

2. Постанова КМ України № 373 від 26.03.2006 „Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах”.

3. Антонюк А. Загрози інформації і канали витоку / А. Антонюк, В. Жора // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – Вип. 2. – С. 42–46.

4. Домарев В. В. Безопасность информационных технологий. Системный подход / В. В. Домарев. – К.: ООО „ТИД” „ДС”, 2004. – 992 с.

5. Поповский В. В. Защита информации в телекоммуникационных системах: Учебник/ В. В. Поповский, А. В. Персиков. – Х.: ООО „Компания СМИТ”, 2006. – 238 с.

МЕТОДИКА КЕРУВАННЯ ТРАЕКТОРІЄЮ БПЛА В АВТОНОМНОМУ РЕЖИМІ ПОЛЬОТУ НА ОСНОВІ НЕЙРОМЕРЕЖЕВОГО АЛГОРИТМУ MELM – MADGWICK

У зв'язку із тим, що у військовій сфері перевага надається мініатюрному класу безпілотних літальних апаратів (БПЛА) через: високу мобільність, дешевизну, легкість маскування, високу маневреність, зростає необхідність розробок алгоритмів інтелектуальних систем управління БПЛА в автономному режимі польоту незалежно від наявності сигналів глобальних систем позиціонування.

Результат експериментів показав, що застосування алгоритму на основі ELM – Kalman точність навчання нейромережі безплатформної інерціальної навігаційної системи (ІНС) була кращою в порівнянні з алгоритмом MELM – Madgwick на 13.94%, та WANN – RNN – Madgwick на 29.82 %. Однак, необхідно зазначити, що точність навчання покращувалась із зростанням кількості нейронів в структурі прихованого рівня < 500 , що підвищує обчислювальну складність та відповідно збільшує час процесу навчання.

Застосування розробленої методики керування траєкторією БПЛА в автономному режимі польоту на основі нейромережевого алгоритму MELM – Madgwick дозволило здійснити адаптацію структури прихованого рівня, яка становить 100 нейронів прихованого рівня, що дозволяє його використання у якості компромісного варіанту, що підтверджено імітаційним моделюванням.

Таким чином, розроблена нова методика керування траєкторією БПЛА в автономному режимі польоту на основі нейромережевого алгоритму MELM – Madgwick, дозволяє:

по-перше, інтегрувати розроблений алгоритм в системи управління БПЛА на базі МЕМС технології мікрокомп'ютерів Arduino Nano, під час зникнення GPS сигналу, на часовому інтервалі $t = (10...300 \text{ с})$, що являється критичним для класу мікро – та малих безпілотників;

по-друге, розроблений алгоритм MELM – Madgwick дозволяє апроксимувати, та екстраполювати вхідні сигнали навігаційних параметрів в динамічному середовищі, за рахунок процесу адаптивного навчання в реальному часі (оптимізації нейромережевої структури);

по-третє, вперше було запропоновано застосувати блок перетворювача навігаційних даних в кватерніону форму для зменшення розмірності вхідних даних, без застосування процесу квантування;

по-четверте, вперше був застосований нейромережевий алгоритм MELM для вирішення задач автономної навігації для зменшення відхилення БПЛА від цільової траєкторії під час зникнення GPS сигналів;

в результаті застосування методики керування траєкторією БПЛА в автономному режимі польоту на основі нейромережевого алгоритму MELM – Madgwick під час зникнення сигналів глобальних супутникових систем позиціонування, похибка прогнозування навігаційних параметрів траєкторії найменша і склала $\approx 30\text{--}33 \text{ м}$, що додатково підтверджує доцільність його використання для мікро - БПЛА.

Напрямок подальших досліджень є розробка методики управління міні – БПЛА в мережах FANETs (Flying Ad-hoc Networks) з урахуванням особливостей організації каналів управління і зв'язку.

ВИКОРИСТАННЯ ДЕЦЕНТРАЛІЗОВАНИХ ТЕХНОЛОГІЙ ДЛЯ ЗАСОБІВ АВТЕНТИФІКАЦІЇ АВТОМОБІЛЯ

У сучасному світі, коли використання електронних систем автентифікації є дуже розповсюдженою технологією в багатьох сферах життя суспільства, деякі з них знаходяться у вжитку вже достатньо великий час, через це вони з часом втрачають свою захищеність та стійкість до атак. Розглянемо детальніше сучасну та критичну до безпеки проблему захищеності сучасних автомобільних систем. Основною проблемою захищеності автомобільних систем є недостатня захищеність системи автентифікації, що дозволяє власникам отримувати доступ до транспортного засобу (фізичний доступ, доступ до програмних елементів для спрощеного використання), вразливості яких можуть привести до отримання доступу зловмисниками.

Основною проблемою систем безпеки є те, що вони побудовані на вже відомих світу технологіях, але дещо спрощених, наприклад використовуються криптографічні системи з зменшеним розміром блоків та ключів, крім того навіть дорогі та складні системи будуються на основі одного центрального серверу, з'єднання з яким може бути скомпрометовано. Було розглянуто можливість використання децентралізованих технологій для покращення рівня захищеності засобів автентифікації, визначено що найкращим рішенням є використання технології блокчейн для покращення рівня довіри та мінімізації можливостей з перехоплення та модифікації даних. Використання технології блокчейн в системі автентифікації автомобіля дозволить розширити можливості безпеки автентифікації для доступу до автомобіля, роблячи цей процес в той самий час простішим для користувача, бо всі дії можна виконувати за допомогою смартфона, що працює на широко відомій платформі, але ж і водночас підвищується рівень безпеки та довіри, не вимагає додаткових грошових вкладень, є легким до налаштування та використання, та є гарно захищеним як від поствантових атак, так і від інших видів атак, що зараз є дуже загрозливими для безпеки сучасної автоіндустрії. Також великим плюсом є те, що Apple буде співпрацювати з виробниками автомобілів для CarKey, та є велика вірогідність виконання версії заводського варіанту, що зробить цю технологію ще більш доступною, простою для потенційних користувачів. Водночас системи безпеки автомобіля будуть мати гарний рівень безпеки автентифікації, для реалізації якої використовується децентралізована мережа блокчейн з вузлами для кожного автомобіля, що автентифікують користувача групово та 51% інших вузлів має підтвердити запит на автентифікацію, в іншому випадку автентифікація буде неможлива і доступу до транспортного засобу надано не буде. Таким чином вирішуються проблеми автентифікації та безпечності передачі даних між блоками між собою, що перетворює розроблену систему в покращений та більш надійний захід автентифікації на основі децентралізованої мережі блокчейн та двох комплексних оновлених схем системи передачі критичних даних всередині автомобіля.

Метою статті є аналіз захищеності систем автентифікації автомобіля та покращення рівня захищеності системи автентифікації автомобіля. Об'єктом інформаційної діяльності є абстрактний транспортний засіб, що використовує для захисту від несанкціонованого доступу систему безпеки високого класу з постійним моніторингом стану захищеності транспортного засобу за допомогою GSM зв'язку, використовуючи який дані відправляються на центральний сервер, до якого може отримати доступ власник для перегляду стану захищеності автомобіля у вигляді веб-сервісу, або з використанням програмного забезпечення, що встановлюється на смартфон.

Сучасні автомобілі є складною мережею, що складаються з багатьох незалежних вбудованих обчислювальних систем, з'єднаних по мережі. Наприклад, автомобіль, що розглядається, складається з понад 200 мікропроцесорів, на яких працює до 65 мільйонів рядків коду, що робить його одним з найскладніших програмних систем. Як і у випадку з

будь-якою складною системою програмного забезпечення, збереження безпеки є актуальною задачею. Вимоги безпеки, що висувуються до компонентів системи автентифікації – це вимоги цілісності, доступності та достовірності, оскільки для правильної роботи всіх системи безпеки автомобіля необхідно щоб інформація, що курсує в ІС, залишалася завжди доступною і цілісною та була не скомпрометованою, бо це є дуже важливим аспектом для правильного керування параметрами безпеки автомобіля та взагалі правильного функціонування всіх його систем. В даній мережі циркулюють критичні дані у вигляді пакетів, що курсують від одного компонента системи до іншого, таким чином компоненти зв'язані між собою та можуть взаємодіяти, що дозволяє автомобілю рухатися та ефективно використовувати системи керування та безпеки. Інформаційна система являє собою мікроконтролер з встановленими додатковими модулями зв'язку з мережею GSM та інтеграції пристрою до мережі CAN. Система побудована на основі клієнт-серверної архітектури, що складається з мікроконтролера з доступом до мережі Інтернет, сервера, що виконує роль системи зберігання даних, що курсують в системі, системи моніторингу даних для виявлення проблем безпеки і загроз, що у випадку позаштатної ситуації відправляє повідомлення на смартфон власника транспортного засобу. У системі безпеки, що встановлений на об'єкт інформаційної діяльності в якості криптографічного захисту інформації використовується KeeLoq, блоковий шифр, заснований на програмному компоненті "NLFSR", що являє собою регістр зсуву з нелінійним зворотним зв'язком. Односпрямований протокол передачі команди був розроблений Фредеріком Брувер, який є генеральним директором компанії Nanoteq Pty Ltd.

Алгоритм KeeLoq був розроблений в середині 80-х Джідеоном Куном з кремнієвої реалізацією Вілліама Сміта в Nanoteq Pty Ltd (підрозділ Південної Африки) і був проданий Microchip Technology, Inc. в 1995 році за 10 млн доларів. Алгоритм являє собою «плаваючий код», кодується і декодується за допомогою мікросхем NTQ105 / 106/115 / 125D / 129D і HCS2XX / 3XX / 4XX / 5XX.

Шифрування відбувається блоками по 32 біта з використанням 64 бітного ключа, один блок тексту шифрується за 528 раундів.

Об'єкти системи безпеки автомобіля, що підлягають захисту:

Система зберігання даних автентифікації, що знаходяться в блоках автомобіля. Система зберігання даних автентифікації, що знаходяться на пристрої власника/того кому він делегує свої обов'язки. Дані автентифікації, дані власника, інформація про машину та її статут, що передаються за допомогою мережі Інтернет.

Засоби захисту інформації, що пропонуються:

Пропонується використання децентралізованої системи блокчейн на заміну клієнт-серверній архітектурі, що дозволяє: не використовувати сервер для зберігання даних про автомобіль, про стан його безпеки, геопозицію та даних автентифікації, що дозволяє ускладнити доступ до перехоплення та модифікації даних на сервері при отриманні неправомірного доступу, оскільки такими серверами в системі блокчейн можна назвати ноди мережі, які й мають виконувати весь функціонал серверів з клієнт-серверної архітектури; важко відстежити ноди мережі, щоб отримати до них неправомірний доступ та мати можливість впливати роботу системи з боку підтвердження невалідних дій від зловмисників та виконати DDoS атаку, бо дані про мережу не відомі; планується встановлена кількість нодів в мережі в кількості 10, що будуть працювати в будь-якому разі, оскільки будуть підтримуватися в робочому стані автоматичним менеджером нод, який має слідкувати за станом мережі та правильністю роботи системи, таким чином забезпечується постійний пул арбітруючих пристроїв, що повинно забезпечити безпечну роботу мережі блокчейн.

Криптографічний захист даних, що дозволяє вирішити проблему щодо атак на зміну цілісності даних, унеможливує підміну даних та перехоплення важливих даних про роботу системи: шифрування даних, що зберігаються в блоці безпеки автомобіля; шифрування даних, що передаються в мережі; валідація даних, що передаються в мережі за допомогою геш-значень; використання захищених каналів зв'язку.

З використанням мережі блокчейн в якості мережі для передачі даних стає можливим використання механізмів керування доступом, що дозволяє ефективно захищати інформацію, що курсує в системі безпеки автомобіля, даних ідентифікації, що передаються та їх верифікації за рахунок відсутності сервера, що може бути скомпрометованим та надійних засобів криптографічного захисту інформації. В якості міток доступу використовується мобільний пристрій з достатнім рівнем довіри (в огляду на те, що криптоконтейнер, що пропонується використовується для зберігання даних банківських рахунків та іншої критичної інформації) з додатковим шифруванням блоковим симетричним шифром «Калина», що є шифром державного стандарту та показує достатню стійкість для такої розробки. У ході роботи була розглянута побудова захищеної системи автентифікації для автомобільних систем, розглянута структура та будова комерційних пропозицій засобів безпеки для безпечної автентифікації власника автомобіля. Визначені можливі загрози зі сторони злоумисників для системи автентифікації автомобіля, найнебезпечніші з цих загроз – модифікація даних, можливість проведення реплей атак, використання вразливих місць у коді мережі та зламування криптоалгоритмів. Була розроблена програмна реалізація тестової моделі систем безпеки з використанням функціоналу моделювання розглянутих в даній роботі видів атак. Програмне моделювання роботи системи автентифікації дозволяє розглянути всі етапи роботи мережі системи, розглянути механізм генерації даних, їх синхронізації між собою, перевірки валідності даних та можливостей з їх модифікації. Було розглянуто можливість впливу на дані автентифікації, що передаються, за допомогою MITM атаки, що дозволило зрозуміти захищеність каналу передачі даних. Метою атаки було скомпрометувати дані, що зберігалися в попередніх блоках, але за рахунок перевірки блоків з використанням геш-значень попередніх блоків, що зберігаються в наступних блоках в блокчейні. Були проведені тести атак на відключення вузлів автентифікації з мережі з використанням атаки DDOS, що повинна була перешкодити роботі мережі через виключення вузлу з мережі, але завдяки тому, що всі вузли були синхронізовані то атака була неефективною, атаки на отримання контролю над 51% блоків для нав'язування даних, що курсують в мережі, але навіть при невеликій кількості блоків, що тестувалися в цій атаці, вона стала ймовірною, коли злоумисником було отримано доступ до двох з трьох вузлів, та той отримав можливість робити нав'язування даних, але в той же час третій блок перестав потрібним чином працювати через те що не була пройдена перевірка валідності блоків, що не змогли засинхронізуватися з скомпрометованими блоками. Таким чином, можна визначити, що розроблена програмна модель системи автентифікації автомобільної системи задовольняє вимогам, висунутим під час розгляду захисту від атак. Були представлені вимоги до рівня безпеки для безпечного використання систем автентифікації та пропозиції щодо досягнення відповідного рівня безпеки з використанням мережі блокчейн, розглянуті можливі загрози для системи безпеки при використанні в якості системи передачі даних мережу блокчейн.

За отриманими даними висунуті пропозиції щодо безпечного застосування технології блокчейн з огляду на розглянуті можливі атаки на реалізації мережі блокчейн.

Об'єктами системи безпеки автомобіля, що підлягають захисту є: система зберігання даних автентифікації, що знаходяться в блоках автомобіля; система зберігання даних автентифікації, що знаходяться на пристрої власника/того кому він делегує свої обов'язки; дані автентифікації, дані власника, інформація про машину та її статут, що передаються за допомогою мережі Інтернет. У ході роботи була розглянута побудова захищеної системи автентифікації для автомобільних систем, розглянута структура та будова комерційних пропозицій засобів безпеки для безпечної автентифікації власника автомобіля. Програмне моделювання роботи системи автентифікації дозволяє розглянути всі етапи роботи мережі системи, розглянути механізм генерації даних, їх синхронізації між собою, перевірки валідності даних та можливостей з їх модифікації. Розроблена програмна модель системи автентифікації автомобільної системи задовольняє вимогам, висунутим під час розгляду захисту від атак.

МОДУЛЬ ЦЕНТРАЛІЗОВАНОГО ЗБЕРІГАННЯ ТА ОБРОБКИ ДАНИХ ІНФОРМАЦІЙНОЇ СИСТЕМИ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ АБОНЕНТІВ СЛУЖБ ТЕХНІЧНОЇ ПІДТРИМКИ

Актуальність теми. Сучасний етап автоматизації управління характеризується стрімким розвитком систем розподільної обробки даних, що дає змогу прискорити обробку інформації за рахунок максимального наближення засобів обробки даних до місць її виникнення, задовільнити різноманітні потреби управлінського персоналу, забезпечити застосування рішень до об'єктів оперативного управління, знизити розміри витрат на утримання обчислювальної системи, збільшити гнучкість і підвищити життєздатність системи, виконавцям безпосередньо брати участь у процесі управління і підвищувати їх відповідальність.

Мета роботи: підвищити ефективність роботи систем технічного обслуговування військових підрозділів за рахунок впровадження інформаційної системи для автоматизації внутрішніх процесів.

Інформаційна система відповідає за прийом, реєстрацію заявки в системі обліку заявок, визначення пріоритету заявки, підтвердження якості проведення заходів з технічної підтримки у абонента (користувача) який оформив заявку. Оформлення заявки з метою отримання послуги з технічної підтримки здійснюється в електронному вигляді через оформлення заявки в системі обліку заявок на головній веб-сторінці автоматизованої системи управління „Дніпро” (далі – АСУ „Дніпро”) або за телефонним номером. В рамках технічної підтримки відкритого телефонного зв'язку здійснюється підтримка пристроїв телефонного зв'язку, ліній зв'язку. Підтримуване обладнання включає в себе аналогові і цифрові АТС, ІР-телефонію, телефонію в мережах ЗСОІ, МОСІ, голосові шлюзи.

Програмний додаток розроблено мовою JavaScript з використанням системи управління контентом Strapi (рис. 1). Strapi дозволяє швидко розробляти API для роботи з даними і займає проміжне положення між фреймворком для Node.js і CMS без користувацького інтерфейсу. Для запуску серверного додатку сервер підтримує середовище виконання серверних JavaScript-додатків Node.js та систему управління базами даних MongoDB. Оптимальним архітектурним рішенням є використання бібліотеки React, транспілятора Babel та бандлера Webpack. Для вихідного коду вебклієнта використовується Apache HTTP.

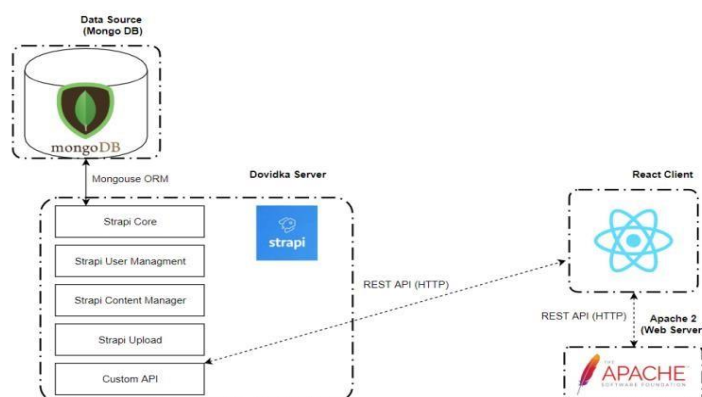


Рис. 1. Схема інформаційної системи

Отже застосування описаної у роботі інформаційної системи дозволить користувачам автоматизувати процес технічного обслуговування підрозділів Збройних Сил України.

АВТЕНТИФІКАЦІЯ КОРИСТУВАЧА ІНФОРМАЦІОНОЇ СИСТЕМИ НА ОСНОВІ ПОВЕДІНКОВОЇ БІОМЕТРІЇ ІЗ ВИКОРИСТАННЯМ НЕЧІТКОЇ ЛОГІКИ

В умовах постійно зростаючої залежності сфери діяльності органів військового управління (ОВУ) від обробки даних у сучасному технологічному режимі, надійність і безвідмовність інформаційних систем (ІС), а також якість інформації набувають першочергового значення. Тому, залишається відкритим питання підвищення рівня кібербезпеки ІС ОВУ.

Одним з актуальних напрямків вирішення даного питання є завдання захисту ресурсів та сервісів ІС від несанкціонованих втручань у руслі забезпечення точного та достовірного визначення автентичності користувача. Існує чотири основні напрямки автентифікації: парольна, комбінована, багатофакторна та біометрична.

Парольна автентифікація є найбільш поширеним простим і звичним методом, головним недоліком якого є залежність його надійності від складності обраних користувачами паролів (занадто короткі паролі, загальновідомі сполучення символів і т.д.).

Комбіновані та багатофакторні методи автентифікації не забезпечують захисту від крадіжки облікового запису, проте надають більш надійний захист, на відміну від використання першого підходу. Системи біометричної автентифікації в свою чергу узагальнено поділяються на два класи: статичні і динамічні (поведінкові). Статична автентифікація ґрунтується на використанні фізіологічних характеристиках людини, тобто унікальній властивості (відбиток пальця, форма обличчя, сітківка ока). Основною перевагою статичної біометрії являється її незалежність від психологічного стану користувача та досить малі затрати на реалізацію. Поряд з цим, апаратна складність таких методів призводить до великих фінансових затрат. Динамічна автентифікація відображає особливості характерних для людини швидких підсвідомих рухів в процесі відтворення контрольного слова рукописним почерком, набору тексту на клавіатурі, або в процесі вимови контрольного слова голосом. Перевагою поведінкової біометрії являється її досить низька вартість і можливість аудиту психофізичного стану користувача ІС.

Для ефективного забезпечення захисту ІС від несанкціонованого доступу пропонується:

побудова профілю користувача шляхом визначення для нього закономірних та притаманних поведінкових характеристик із усього набору можливих (наприклад для клавіатурного почерку – швидкість друку, кількість задіяних пальців для набору, кількість помилок при наборі, інтервали між натискання на клавіші, час утримання клавіші, ступінь аритмічності при наборі, кількість помилок при наборі і т.д.);

здійснення періодичного визначення автентичності користувачів протягом усієї сесії роботи з ІС на основі встановлення рівня відповідності їм попередньо побудованого профілю із використанням апарату нечіткої логіки.

Даний підхід на відміну від відомих, дозволить позбутися залежності від психоемоційного стану користувача шляхом інженерії о закономірностей із набору досліджуваних параметрів, здійснювати аналіз в умовах неповноти та нечіткості управляючої інформації, а також автоматично будувати правила для нечіткої системи логічного виводу на основі знайдених закономірностей у вигляді шаблонів (правил), що у свою чергу дозволить вирішити питання суб'єктивного судження експертів.

Таким чином, можна зробити висновок про доцільність застосування поведінкової біометрії із використанням нечіткої логіки в системах контролю доступу до ІС на етапі визначення автентичності заявленого користувачем ідентифікатора, що значно сприятиме підвищенню рівня кібербезпеки ІС ОВУ.

МОДЕЛЬ ІНТЕГРОВАНОЇ СИСТЕМИ МОНІТОРИНГУ НАДВОДНОЇ ОБСТАНОВКИ В МЕЖАХ ВИКЛЮЧНОЇ (МОРСЬКОЇ) ЕКОНОМІЧНОЇ ЗОНИ УКРАЇНИ

Україна має вихід в Чорне та Азовське моря. Відповідно до Закону України «Про державний кордон» охорону морських кордонів України здійснює Державна прикордонна служба України та Збройні Сили України. Також завдання щодо правомірності використання територіальних вод та морського шельфу України стоять перед правоохоронними органами України, Державним агентством рибного господарства та Міністерством захисту довкілля та природних ресурсів України.

В результаті проведеного аналізу встановлено, що охорона територіальних вод та морського шельфу України здійснюється з стаціонарних постів спостереження, мобільних постів спостереження, а також із використанням морських та повітряних суден. Так, для охорони морських кордонів України використовуються наступні технічні засоби: тепловізійні комплекси, оптико-електронні системи спостереження, радіолокаційні станції, станції прийому даних системи АІС, плавзасоби, безпілотні авіаційні комплекси, патрульна авіація, відкриті онлайн ресурси контролю надводної обстановки тощо.

Зазначені засоби дозволяють ефективно реалізовувати завдання щодо забезпечення охорони морських кордонів України на відстані до 40 км від узбережжя. Однак, Конвенцією ООН з морського права (UNCLOS 1982) визначено, що максимальна ширина виключної (морської) економічної зони держави, що має морські кордони, може простягатися на відстань до 200 морських миль від узбережжя (близько 370 км), що значно перевищує зазначену відстань.

Враховуючи протяжність морського кордону (1355 км), ширину виключної (морської) економічної зони (370 км), агресивні дії Російської Федерації в акваторії Чорного та Азовського морів, тимчасову окупацію Кримського півострова, наявні сили та засоби Державної прикордонної служби та Військово-морських сил України, можна прийти до висновку, що ефективного забезпечення моніторингу виключної (морської) економічної зони України на даний час є ускладненим.

У зв'язку з цим, існує необхідність розробки та побудови інтегрованої системи моніторингу надводної обстановки в межах всієї виключної (морської) економічної зони України, яка б дозволяла оперативно отримувати інформацію про: переміщення військових та урядових суден, незаконний рибний промисел, незаконну розробку континентального шельфу, порушення міжнародних правил судноплавства, обхід судновласниками міжнародних санкцій тощо.

Вирішення даної задачі можливе через комплексування даних з різних джерел. Зокрема, пропонується здійснювати поєднання даних дистанційного зондування Землі з даними, отриманими в рамках моніторингу радіоелектронної обстановки, оптико-електронного спостереження, а також даними систем ідентифікації та контролю місцезнаходження суден.

Реалізація зазначеної моделі сприятиме зміцненню обороноздатності та захисту національних інтересів України в межах виключної (морської) економічної зони.

РЕКОМЕНДАЦІЇ ЗІ СТВОРЕННЯ СПЕЦІАЛІЗОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ РОЗРАХУНКУ СИСТЕМИ ІНЖЕНЕРНИХ ЗАГОРОДЖЕНЬ

Актуальність. У відповідності до стратегічних цілей Державної програми розвитку ЗС України одним із ключових завдань є удосконалення системи управління. Напрямок досягнення є створенням єдиної інформаційної системи управління оборонними ресурсами.

Ведення сучасних бойових дій неможливо без ефективного управління військами. За усталеним визначенням управління – це процес цілеспрямованого впливу командувачів (командирів), штабів на війська, що здійснюється для підтримки готовності військ до виконання завдань за призначенням, їх підготовки та успішного виконання ними завдань у ході ведення операції (бойових дій).

Враховуючи всі особливості ведення збройної боротьби в сучасних умовах, необхідно виділити основне протиріччя у сфері управління військами – між зростаючими обсягами інформації та зменшенням часу, що є в наявності в органів управління для її збору, обробки і доведенням до командувача (командирів) необхідної інформації з метою прийняття раціонального, обґрунтованого рішення. Розв'язання цього протиріччя полягає у значному підвищенні оперативності процесу збору, обробки і доведенні інформації, що забезпечить підвищення оперативності управління в цілому.

Постановка задачі. Проведений аналіз показує, що у 2016 році рівень автоматизації діяльності органів управління становив лише 10 – 30 % від потреб, наявні системи, засоби не складали цілісних систем, існуючі інформаційно-розрахункові задачі відповідали потребам пунктів управління лише на 12 – 15 %, у зв'язку з чим керівному складу для вироблення та прийняття рішень залишалося тільки 17 % часу від циклу управління на відміну від 75 – 80 %, що є характерним для збройних сил передових країн світу.

Мета. Досвід проведення АТО, ООС показує, що практично відсутність автоматизованого управління військами дуже суттєво знижує ступінь реалізації бойових можливостей військ (сил). Однак окремі елементи єдиної автоматизованої системи управління збройними силами типу „Дельта”, „Кропива” вже використовуються.

Аналізуючи ведення локальних війн і збройних конфліктів останніх років, слід зазначити, що відбуваються значні зміни в теорії їхнього оперативного забезпечення та, зокрема, інженерного забезпечення сучасних бойових дій. Окреме місце при цьому займає створення, перш за все, ефективної системи інженерних загороджень (СІЗ).

Одним із етапів підвищення ефективності СІЗ є оптимізація процесу планування СІЗ, які можуть бути реалізовані за допомогою методів оптимізації, а саме через програмне (математичне) моделювання.

Основні положення. Слід зазначити, що однією із складових мети управління військами є забезпечення визначеного рівня бойової готовності військ, їх всебічна підготовка до застосування та ефективна реалізація оперативних (бойових) можливостей військ у ході ведення операцій (бойових дій). Тому досягнення зазначеної вище мети можливо здійснити через процес оптимізації, як системи управління в цілому, так і зокрема її складових.

Ймовірним варіантом досягнення мети на даному етапі, є створення спеціалізованого програмного математичного забезпечення для розрахунку СІЗ, яке в подальшому повинно стати невід'ємною складовою єдиної автоматизованої системи управління військами.

З метою забезпечення успішного функціонування програмного продукту СІЗ створюється багаторівнева база даних до якої входять: часові показники, основні завдання інженерного забезпечення, детальні відомості про сили, засоби, як противника, так і про свої війська тощо.

Загальний алгоритм роботи спеціалізованого програмного математичного забезпечення являє собою ряд взаємопов'язаних деталізованих інструкцій, що реалізують процес обчислення, який, починаючи з початкового стану, відбувається через послідовність

логічних станів та завершується кінцевим. Перехід з попереднього до наступного стану не обов'язково детермінований – деякі алгоритми можуть містити елементи випадковості.

При введенні інформації (завдань), для прикладу з контрмобільності підрозділів противника. Кінцевим результатом обчислення є формування висновку щодо можливостей (спроможностей) своїх підрозділів виконати визначене бойове завдання.

Важливим етапом формування вихідних даних є цифрове відображення на дисплеї планшета (ПЕОМ) детальної обстановки, що склалася, відомостей про противника та свої війська, особливо про їх інженерні заходи. Далі, відповідно до замислу (рішення) загальновійськового командира, на цифровій карті (схемі) виводяться задані щільності інженерних загороджень (ефекти), яких повинні будуть спочатку досягти на етапі планування СІЗ.

СІЗ формується шляхом нанесення на цифрову карту по елементах різноманітних інженерних загороджень з урахуванням „доступності” для дій військ противника. Програма дає можливість при збільшенні (зменшенні) форми об'єкта, отримувати відомості про його протяжність, глибину, витрату боєприпасів, ймовірність ураження, час затримання тощо. При цьому оператором обов'язково задаються такі відомості як: ефект загородження, тип боєприпасів, спосіб виконання завдання, сили, засоби механізації, умови виконання та ін.

Результатом опрацювання наведених вище даних є надання пропозицій щодо спроможності підрозділу виконати визначене завдання, потреба у додатковому оснащенні засобами, пропонується схема улаштування загородження для досягнення заданого ефекту, а також визначаються щільність загороджень їх координати, які у свою чергу доповнюють базу додаткових можливостей програми. До них належить: внесення відомостей до „Е-формуляру” загороджень, коригування їх у ході проведення рекогносцирувальних робіт, передача інформації до вищих штабів, а також внесення змін у ході виконання завдань в умовах реального часу тощо.

Слід зазначити, що в ході передачі даних з одного рівня до основної бази даних, оператором вводяться умови ведення бою (операції) з обов'язковим врахуванням різноманітних коефіцієнтів, серед яких чільне місце займає „коефіцієнт реальності”, який враховує поступове зменшення можливостей підрозділів. Після чого на інтерфейс користувача виводиться інформація про витрату засобів інженерного озброєння, майна, визначається потреба у машинорейсах, пальному тощо.

На основі опрацювання усіх даних визначається бойова ефективність інженерних загороджень, яка характеризується наступними кількісними показниками як: ураження техніки, живої сили, а також зменшення темпу просування противника та ін.

Результатом оброблення даних на завершальному етапі, є формування ряду пропозицій, які надаються на затвердження старшому командиру (начальнику). Також, у разі виявлення обмежених можливостей підрозділів з виконання завдань по створенню СІЗ (визначених щільностей), передбачено функцію щодо додаткового залучення необхідних сил і засобів старшого начальника. При підтвердженні запиту, вони вносяться до загальної бази даних.

Після затвердження командиром пропозицій, наданих начальником інженерної служби (відділу групи), здійснюється їх доведення до підпорядкованих підрозділів через систему засобів комунікації.

Також, слід зазначити, що даним питанням у збройних силах держав-членів Північноатлантичного альянсу приділяється значна увага протягом тривалого періоду часу. Заслужує уваги ряд розрахункових програм типу „Engineer asset calculation”, „ЕС” та ін., які спрощують процес планування операцій офіцерами штабу НАТО на відміну від роботи офіцерів штабу ЗС України.

Висновки. Таким чином, впровадження рекомендацій щодо розроблення спеціалізованого програмного математичного забезпечення, дозволить скоротити час на проведення розрахунків до 25 %. А також підвищить кількість можливих варіантів створення СІЗ до 10 %.

ПРОБЛЕМА КІБЕРБЕЗПЕКИ В ОСВІТНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЯХ

Постановка завдання. На даний час спостерігається активізація захист наукових робіт в тому числі дисертаційних за напрямком інформаційні технології в частині розробок їх для забезпечення гармонізації вищої освіти. Аналіз таких робіт, наприкладі, [1] на при велике здивування було не побачити висвітлення аспекту щодо забезпечення кібербезпеки зазначеної системи.

Тому, на нашу думку виникла необхідність в доповіді обговорити окремі аспекти забезпечення кібербезпеки інформаційних систем та технологій, що пропонуються в освіті.

Мета доповіді. Апробувати ідеї щодо необхідності забезпечення кібербезпеки інформаційних систем та технологій в освіті.

Результат дослідження. Для рішення кібербезпеки інформаційних систем та технологій в освіті розглянемо найбільш чітке з методологічної точки зору тлумачення дефініції „інформаційної технології”.

Згідно ДСТУ 2392-94 [2] „інформаційна система” – це комунікаційна система, що забезпечує збирання, пошук, оброблення та пересилання інформації.

Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” визначає інформаційну (автоматизовану) систему як організаційно-технічну систему, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів [3].

Згідно ISO/IEC 2382:2015 [4] „информационная система – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т.д.), которые обеспечивают и распространяют информацию”.

Отже, інформаційна технологія – це сукупність методів, засобів, прийомів, що забезпечують пошук, збирання, зберігання, опрацювання, подання, передавання інформації між людьми.

Інформаційні технології – це процеси, які реалізуються засобами обчислювальної техніки і забезпечують виконання заданих вимог до пошуку, подання, перетворення та передавання інформації, тобто процеси, що реалізують інформаційну діяльність людини. Схематично складові інформаційної технології за джерелом [5] подана на рис 1.

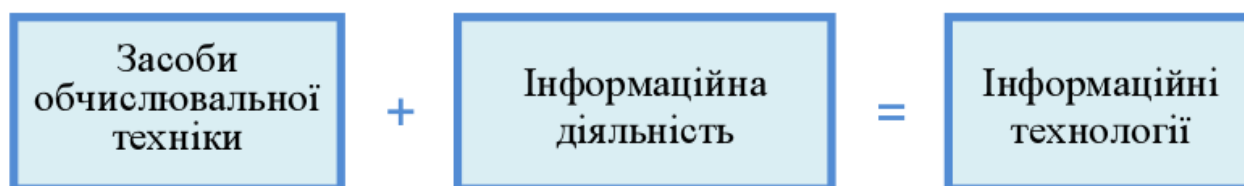


Рис. 1. Складові класичної інформаційної технології

Основними компонентами інформаційної технології навчання є технічні засоби (персональний комп’ютер, засоби мультимедіа та ін.), програмні засоби та організаційно-методичне забезпечення.

Оскільки основою технологічного процесу навчання є отримання і перетворення інформації, то будь-яку педагогічну технологію можемо назвати інформаційною. Новітніми інформаційними технологіями навчання в широкому сенсі прийнято називати процес підготовки і передачі інформації до учня за допомогою відповідних компонентів цих технологій і в першу чергу – персонального комп’ютера.

Із вище розглянутих означень інформаційні технології є алгоритмічною основою побудови та функціонування інформаційних систем. Іншими словами функціонування інформаційної системи, яка забезпечує збирання, пошук, оброблення та пересилання інформації здійснюється по розробленим і затвердженим методами, засобами, прийомами, що забезпечують пошук, збирання, зберігання, опрацювання, подання, передавання інформації між людьми. Як свідчить сучасна практика інформаційні системи вразливі до деструктивних інформаційних впливів (кібервпливу).

Можливі наступні комбіновані варіанти кібервпливу:

- 1) сукупність зовнішнього та внутрішнього впливу;
- 2) внутрішнього впливу;
- 3) зовнішнього впливу.

Кібербезпека від зовнішнього впливу забезпечується якщо інформаційна система в освіті (ІСО) що застосовує розроблену інформаційну технологію в освіті (ІТО) працюють в автономному режимі, тобто без можливості зовнішнього втручання в її роботу. Ця норма відразу втрачається з бажанням застосуванням дистанційного керування на базі платформи іноземного виробництва, наприклад мережі Інтернет.

Щодо внутрішнього впливу, то джерелом його походженням як правило є людина-інсайдер. Технічні збій ми опускаємо розгляд, оскільки вони більше пов'язані з технічною надійністю технічних засобів, що реалізують інформаційну систему. Практика показує, що вже через 5 років експлуатації комп'ютерів, внаслідок морального старіння, доцільно замінювати їх на новіші, хоча фізичне старіння або знос їх далекі від граничного стану. Це пов'язано з тим, що крива морального старіння об'єкта перетинає і перевищує гранично допустимий рівень показника ціна/якість і, отже, подальша його експлуатація нерентабельна [6].

Ми не говоримо поки що про необхідність будувати повноцінну комплексну систему захисту інформації (КСЗІ), але необхідно додержуватися (забезпечувати) елементарну кібербезпеку (кібергігієну) при поводженні у кіберпросторі.

Висновки. Таким чином, із інтенсифікацією розробок і застосувань інформаційних систем та інформаційних технологій в освіті необхідно:

обговорити окремі аспекти забезпечення кібербезпеки;

рекомендувати в наукових роботах освітлювати заходи забезпечення кібербезпеки пропонувані інформаційних систем на основі інформаційних технологій.

Перспективи подальших наукових досліджень. Розробка гібридних інформаційних технологій для застосування науковим керівникам для розвитку методологічної культури у ад'юнктів.

ЛІТЕРАТУРА

1. Цюцюра М.І. Інформаційні технології гармонізації зрівноваженого освітнього простору: автореф. дис. ... д-ра техн. наук : 05.13.06 / Цюцюра Микола Ігорович; Київ. нац. ун-т буд-ва і архітектури. Київ, 2020. 44. с.
2. ДСТУ 2392-94 „Інформація та документація. Базові поняття”. К.: УкрНДІССІ, 1994. 25 с.
3. Закон України „Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994 № 80/94-ВР // Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр>. (дата звернення 28.05.20).
4. ГОСТ 33707-2016 (ISO/IEC 2382:2015) Информационные технологии (ИТ).
5. Носенко Т.І. Інформаційні технології навчання: начальний посібник. – К.: Київ. ун-т ім. Бориса Грінченка, 2011. 184 с.
6. Шубинский И.Б. Структурная надежность информационных систем. Методы анализа. М.: „Журнал Надежность», 2012. 216 с.

ВИКОРИСТАННЯ ОКРЕМОЇ КАТЕГОРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ДЛЯ ОРГАНІЗАЦІЇ ЗВ'ЯЗКУ

На даний час організація зв'язку є актуальним питанням, як у цивільному житті, так і у силових відомствах, не виняток і Збройні Сили України.

Пов'язано це з тим, що у даних структурах зв'язок використовується з метою їх управління, необхідно постійно віддавати накази, розпорядження та ставити відповідні завдання, як в межах однієї військової частини, так і у цілій мережі виду ЗСУ.

В умовах швидкоплинності сучасних війн і збройних конфліктів якісне інформаційне забезпечення бойових дій військ (сил) стає визначальною умовою досягнення стратегічної, оперативної та тактичної переваги над противником.

Це призводить до пошуку нових способів ведення бойових дій, а також організації підтримки військ на полі бою з урахуванням останніх досягнень у галузі інформаційних технологій і телекомунікацій. Саме тому в комплексі заходів щодо забезпечення обороноздатності держави поряд з підтриманням високої бойової готовності військ (сил) пріоритетним напрямком є розвиток і вдосконалення системи військового управління та її технічної основи – системи зв'язку ЗС України, як найважливішого елемента державної та військової інфраструктури, яка визначає ефективність застосування військ та зброї.

Зараз у ЗС України широко використовуються інформаційно-телекомунікаційні системи, які діють у відповідності до наказу МОУ від 01.06.2012 № 372 «Про затвердження Керівництва з технічного забезпечення обладнанням інформаційно-телекомунікаційних систем». З розвитком технічного обладнання постало питання про систематизацію та автоматизацію управління військами, відповідно було організовано низку дослідно-конструкторських робіт, що були спрямовані на вирішення даних питань.

Враховуючи перспективи розвитку слід вказати що дані інформаційно-телекомунікаційні системи будуть використовувати захищені канали передачі даних, проте будь яке середовище має вразливі місця, тому інформація будь-якого типу (виду) може бути скомпрометована.

Відповідно нинішній прогрес розвитку в сфері кібернетики надає чималі можливості щодо підвищення оперативності управління військами незалежно від їхнього базування. До кожної ІТС розроблене відповідне програмне забезпечення що надає йому змогу функціонувати і виконувати ті задачі які стоять перед оператором.

Як вирішення цьому слід розглянути питання розроблення відповідного програмного забезпечення, який би надав змогу підвищити захищеність даних, що передаються. Тобто дане ПЗ має забезпечити надійний захист інформації що безпосередньо підлягає обробці та передачі, відповідно оператор повинен мати чим найменший функціонал даних програм, програми мають бути якомога простішими у реалізації інтерфейсу щоб у оператора не виникало труднощів при роботі і не підризалась оперативність.

Відповідно до способів захисту інформації у середовищі є такі способи як: кодування, шифрування, хешування. Відповідно якщо розглянути середньостатистичне забезпечення по військових частинах, то найбільш сприятливим для реалізації та найменшого навантаження на ІТС буде програма що надає змогу шифрувати інформацію яка буде передана по каналах зв'язку.

На виході ми отримаємо значне підвищення оперативності за рахунок того що оператор повинен буде лише обробити інформацію (ввести її у відповідну програму) без інших операцій. Як висновок з метою підвищення захищеності даних, які підлягають передачі по каналах зв'язку, необхідно використовувати програми (програми-чати) з вбудованим криптоалгоритмом, який надасть можливість зашифровування інформації з відповідно необхідною криптостійкістю та автоматичним генеруванням ключової інформації для мережі в якій відбувається передача даних по відкритих чи захищених каналах зв'язку.

НАПРЯМКИ ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ ДЛЯ ВИЯВЛЕННЯ НОВІТНІХ КІБЕРАТАК

Згідно стратегії кібербезпеки України, одним з пріоритетних напрямків її забезпечення є створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз і створення умов для впровадження в Україні сучасних технологій кіберзахисту. Ефективне вирішення поставлених завдань безпосередньо залежить від розробки та впровадження у діяльність суб'єктів забезпечення кібербезпеки новітніх інформаційних технологій.

Інструменти Data Mining можуть знаходити неочевидні закономірності самостійно і також самостійно будувати гіпотези про взаємозв'язки. Оскільки саме формулювання гіпотези щодо залежності є найскладнішою задачею, перевага Data Mining в порівнянні з іншими методами аналізу є очевидною.

Основні задачі, які вирішуються методами Data Mining:

- класифікація – віднесення об'єктів (спостережень, подій) до одного з заздалегідь відомих класів;
- регресія (в тому числі задачі прогнозування) – встановлення залежності безперервних вихідних від вхідних змінних;
- кластеризація – угруповання об'єктів (спостережень, подій) на основі даних (властивостей), що описують сутність цих об'єктів, у кластери.
- асоціація – виявлення закономірностей між пов'язаними подіями;
- послідовні шаблони – встановлення закономірностей між пов'язаними в часі подіями;
- аналіз відхилень – виявлення найбільш нехарактерних шаблонів.

Усі методи Data Mining поділяються на дві групи за принципом роботи з початковими навчальними даними:

- дані після Data Mining зберігаються - кластерний аналіз, метод найближчого сусіда, міркування за аналогією (традукцією);
- дані деталізуються для подальшої обробки, тобто необхідним є виявлення і використання формалізованих закономірностей або дистиляція шаблонів.

Оцінка стану кібербезпеки об'єктів критичної інформаційної інфраструктури з урахуванням індикаторів кіберзагроз будь якого масштабу є об'єднанням та пошуком кореляції між:

- даними аудиту стану захищеності об'єктів критичної інфраструктури;
- даних щодо оцінки ризиків та моделей кіберзагроз;
- даними про індикатори, що передують відомим кіберзагрозам.

Якість оцінки залежить від наступних факторів:

- визначення основного переліку індексів щодо оцінки кібербезпеки типових для даного об'єкту критичної інфраструктури;
- здійснення збагачення(уточнення) даних моделі шляхом введення регіональних індексів;
- застосування технології великих даних для роботи з структурованими та не структурованими даними;
- здійснення кореляції та виявлення залежностей між індексами (створення шаблону індикаторів);

Висновки. Найбільш перспективним напрямком інтелектуального аналізу в галузі кібербезпеки є методи, які представляють собою множину підходів, об'єднаних ідеєю комп'ютерної математики та використання теорії штучного інтелекту. До основних методів цієї групи належать нейронні мережі, дерева рішень, кластерний та асоціативний аналізи, побудова нелінійних регресій та інші.

ПРОБЛЕМАТИКА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ОПЕРАТИВНОГО РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

Реагуючи на світові тенденції та виклики сьогодення у сфері кібербезпеки Верховна Рада України ввела в дію Закон України “Про основні засади забезпечення кібербезпеки України”. Так, починаючи з 2017 року у інформаційно-правовому просторі нашої держави з’явилася низка законодавчих положень, які визначають 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.

Кібербезпека досягається та забезпечується якісним виконанням сукупності заходів кіберзахисту (організаційних, правових, інженерно-технічних, криптографічного та технічного захисту інформації), які спрямовані на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування об’єктів кіберзахисту. Кіберзахист є сукупністю організаційних, правових, криптографічного і технічного захисту національних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури. Організаційно-технічна модель кібербезпеки є комплексом заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості об’єкта (об’єктів) кіберзахисту.

Доповідь присвячена стислому викладенню проблеми та структурно-логічної схеми дослідження, яке обумовлено практичною необхідністю впровадження підтримки прийняття рішень в процесі оперативного реагування на кіберінциденти, а також стислому викладенню основних наукових результатів.

Модель знань про об’єкт кіберзахисту визначає залежність між значенням показника кіберзахищеності від сукупності ймовірностей виконання елементами об’єкта кіберзахисту обчислювальної роботи, яка обумовлена активізацією програмних алгоритмів реалізації типових класів кібератак. Обґрунтування залежності базується на застосуванні: по-перше, аксіоматичного підходу для встановлення необхідних відношень між елементами множин сутностей “користувач”, “прикладний процес”, “елемент мікропрограмного управління”; по-друге, логічного висновку на основі знання поточного стану аксіоматично введених логічних елементів та зв’язків між ними щодо визначення впливу на показник кіберзахищеності.

Модель захищеності елемента мікропрограмного управління визначає залежність між ймовірністю несанкціонованої зміни налаштувань (логічної структури) елемента мікропрограмного управління від середнього часу обслуговування інформаційного потоку на достатньо широкому раціонально обраному діапазоні варіантів його надходження.

Метод ідентифікації інформаційного напрямку об’єкта кіберзахисту полягає у формуванні унікального образу функціонування відповідної послідовності елементів мікропрограмного управління при передаванні певного варіанту інформаційного потоку на основі автокореляційної функції сукупності середніх значень часу його обслуговування.

Метод виявлення порушень якості інформаційного напрямку комунікації прикладних процесів об’єкта кіберзахисту базується на співставленні фактичних та еталонних результатів, які визначаються за попереднім методом.

Методика оцінювання захищеності є придатною для практичного застосування комплексною реалізацією запропонованих наукових положень.

Висновки. Викладені положення утворюють науково-методичний базис для прототипу комплексу підтримки прийняття рішень оперативного реагування на кіберінциденти в об’єктах кіберзахисту у межах компетенції національних суб’єктів кібербезпеки.

ПРОТИДІЯ „РОЮ” БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ПРОТИВНИКА

В даний час, безпілотні літальні апарати (БПЛА.) Знаходять широке застосування в збройних силах багатьох країн. Можна стверджувати, що скоро це призведе в кінцевому підсумку до створення самостійного роду військ, який буде вирішувати завдання розвідки і нанесення ударів як на тактовному, оперативно-тактовному так і стратегічному рівні управління. При цьому основна увага приділяється застосуванню не поодиноким БПЛА, а їх угруповання або „рою” (UAV Smart) [1 – 3].

Тактика застосування UAV Smart на основі „рою” дозволяє використовувати велику кількість розвідувальних, ударно-розвідувальних і ударних UAV Smart одночасно. Крім того, застосування „рою” дає практично необмежені можливості по веденню розвідки з високою ефективністю, успішно вражати наземні цілі з мінімальними втратами UAV Smart, і найголовніше з мінімальними людськими втратами. Мінімальна величина ефективної площі розсіювання UAV Smart за рахунок його розмірів і покриття істотно знижує ефективність традиційної системи боротьби з UAV Smart. При цьому такі UAV Smart можуть ефективно виявлятися і супроводжуватися тільки телевізійними засобами або засобами візуального спостереження систем протиповітряної оборони, можливості щодо застосування яких сильно залежать від погодних умов.

Це означає, що повністю знищити „рій” БПЛА не представляється можливим. Ситуація, при якій кількість каналів для перехоплення буде збігатися з кількістю БПЛА в складі „рою” є малоймовірною.

Система UAV Smart складається з апаратної частини і програмного забезпечення. Тактика застосування „рою” визначається програмним забезпеченням кожного БПЛА.

Застосування UAV Smart має такі переваги:

- зниження сумарної вартості UAV;
- можливість розподілу корисною (бойовою) навантаження з кількох UAV, при цьому має місце економія вартості апарату з навантаженням;
- зниження вартості втрат в результаті аварій;
- поліпшення точності позиціонування кожного UAV за рахунок взаємного позиціонування кожного з них;
- гнучка тактика застосування.

У той же час застосування UAV Smart має ряд обмежень:

- високі вимоги до бортового обладнання, до обчислювальних можливостей бортового комп'ютера;
- наявність бортовий операційної системи, що працює в реальному масштабі часу.
- можливість зіткнень в умовах створюваних повітряних потоків;
- наявність можливості перерозподілу завдань окремих дільниць „рою”, наприклад, при виході з ладу (знищення) одного або декількох UAV.

Побудова „рою” засноване на ієрархічній структурі. У складі „рою” є БПЛА які здійснюють управління всіма апаратами „рою”. Управління „роєм” здійснюються також через UAV1 Smart які можуть управляти в разі виходу з ладу апаратури управління групою. У свою чергу група ділиться на підгрупи, структура підгрупи аналогічна структурі групи. В її складі є апарати UAV2 Smart які можуть управляти підгрупою в разі виходу з ладу апарату управління підгрупою UAV2. Загальна кількість апаратів в „рої” UAV Smart може бути більше 200. При такій системі управління з наземного пункту здійснюється управління тільки відомими апаратами „рою”.

Як правило таких апаратів може бути кілька. У разі виходу з ладу веденого його місце займає інший UAV Smart подібного типу. У процесі польоту UAV Smart обмінюються інформацією між собою.

В першу чергу це інформації про взаємні відстанях між UAV Smart для запобігання зіткнень, управління польотом і виконання поставленого завдання „роєм”. Обмін такою інформацією може здійснюватися в інфрачервоному, так і в короткохвильовому діапазоні. Таким чином процес польоту угруповання супроводжується випромінюванням кожним UAV Smart „роєм”.

Це означає, що „рій” крім візуальних володіє демаскуючими ознаками в діапазоні роботи. Ця інформація може бути використана протидіючої стороною для боротьби з „роєм”. Боротьба з „роєм” UAV Smart не може бути односторонньою. Це пов'язано в першу чергу великим числом елементів „рою”. З іншого боку, збільшення числа елементів «рою» призводить до зростання демаскуючих ознак.

Таким чином, можна сформулювати основні способи боротьби з «роєм»:

- знищення UAV Smart за допомогою наземних вогневих засобів;
- придушення каналів управління коштами радіоелектронної боротьби

короткохвильового і інфрачервоного діапазону;

- перехоплення каналів управління, наприклад, примусова посадка в обраному місці;
- блокування використання озброєння UAV Smart.

Якщо кількість UAV „рою” велике, то надійне його знищення наземними вогневими засобами неможливо як і здійснення надійного придушення каналів управління.

У цьому випадку найбільш цікавим є використання свого „рою” для знищення «рою» противника. Такий підхід є, на наш погляд, більш перспективним. При цьому слід розглядати перехоплення рою UAV саме за допомогою двох-трьох ешелонів знищення.

Перший і другий ешелон рою перехоплювачів, має завдання значно зменшити щільність рою, та визначити основні напрямки атаки рою. На цьому етапі UAV Smart перехоплювач займає місце для підриву так, щоб впливу зазнали якомога більше UAV Smart рою противника, при цьому досягається мінімальна кількість підриву власних UAV.

Крім того здійснюється, одночасне придушення каналів управління рою противника з метою зниження ефективності застосування рою противника.

Третій ешелон перехоплення рою супротивника має на меті знищення за допомогою індивідуального наведення перехоплювача на UAV Smart „рою” противника.

У перспективі саме трешелона побудова системи перехоплення ударного угруповання БПЛА дозволяє ефективно вирішувати завдання знищення „рою” противника. Перші два ешелону використовуються для зменшення щільності бойового порядку, а третій – для індивідуального перехоплення і знищення.

ЛІТЕРАТУРА

1. Н. Новичков, Д. Федюшко „Рой” беспилотников. Новая тактика боевых действий уникального оружия Китая. 2019 г. [//https://tass.ru/armiya-i-opk/5786857](https://tass.ru/armiya-i-opk/5786857).
2. С. Юфеев. Рой беспилотников. Будущее боевых действий. 12.11.2019 [//https://topwar.ru/164570-roj-bespilotnikov-budushee-boevyh-dejstvij.html](https://topwar.ru/164570-roj-bespilotnikov-budushee-boevyh-dejstvij.html)
3. А. Балаев В США ударный беспилотник запустит целый „рой дронов” 21.04.2020 <https://profile.ru/news/protection/army/v-ssha-udarnyj-bespilotnik-zapustit-celyj-roj-dronov-289675/>

МЕТОДИ ТА ІНСТРУМЕНТИ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ WEB-ДОДАТКІВ

Актуальність. Сучасні інформаційно-телекомунікаційні та комп'ютерні системи (ІТКС) є модульним і відкритим структурами. З одного боку це дозволяє динамічно розвиватися різним інформаційним і мережним технологіям, а з іншого надає базу знань для проведення злочинних дій хакерам. Одним з найбільш дієвих способів протидії зловмисним атакам на ІТКС є здійснення внутрішнього тестування на проникнення (реп-тестування).

Аналіз статистичних даних хакерських зломів, а також проведені дослідження показали, що останнім часом все більше кібератак проводиться на веб-ресурси. Загальна методологія проведення реп-тестування веб-ресурсів описана в документах відкритого проекту забезпечення безпеки веб-додатків (OWASP). Подібна широта поширення і відкритість документації OWASP з одного боку дозволяє динамічно вдосконалити окремі засоби, методики і механізми проведення тестування, але з іншого ускладнює процес формування загальної методології проведення реп-тестування веб-додатків. Вирішенню цього завдання присвячена ця робота.

Мета. Метою роботи є формування загальної методології проведення реп-тестування веб-додатків.

Основна частина. Сучасний веб-ресурс є механізмом, що постійно розвивається, оновлюється і удосконалюється. Ці удосконалення націлені на поліпшення продуктивності, підвищення конверсії, оптимізації роботи і зручності використання.

Але при цьому з тих чи інших причин можуть бути допущені помилки, які можуть призвести до компрометації веб-ресурсу. Це можуть бути «забуті» службові скрипти, недостатній контроль за даними, відсутність перевірок доступу, висновки різних помилок і багато іншого.

Саме тому здійснення планових реп-тестів на веб-додаток є невід'ємним компонентом його успішного та довготривалого функціонування.

Процес реп-тестування веб-додатку включає в себе:

Крок 1: Активна та пасивна розвідка.

Першим кроком у тестуванні є фаза розвідки або збору інформації. Цей крок надає тестувальнику інформацію, яка може бути використана для виявлення та використання вразливостей у веб-додатку.

Пасивна розвідка означає збір інформації, яка легко доступна в Інтернеті, без безпосереднього взаємодії з цільовою системою. Здебільшого це робиться за допомогою Google, починаючи з субдоменів, посилань, попередніх версій тощо.

Активна розвідка, навпаки, означає безпосереднє зондування цільової системи для отримання результату.

Інструментами для здійснення активної розвідки можуть бути: Nmap, Nessus, Nikto, OpenVas, WireShark та BurpSuite, DIRB, theHarvester.

Крок 2: Атака або фаза виконання

Наступним кроком є власне етап експлуатації. На цьому етапі ви здійснюєте атаки на основі інформації, яку ви зібрали на етапі розвідки.

Існує кілька інструментів, якими можна скористатися для атак, і саме тут збір даних відіграє важливу роль. Інформація, яку ви зібрали, допоможе вам зв'язати необхідні вам інструменти відповідно до проведеного раніше дослідження.

Інструментами для здійснення фази виконання можуть бути: Metasploit, Armitage, Hydra, BeEF

Висновок. Було розглянуто сам процес реп-тесту, та інструменти для його реалізації. На основі проведених досліджень стає зрозумілим той факт, що проведення реп-тестів є необхідною умовою в успішному і довготривалому функціонуванні будь-якого web-додатку.

ПЕРСПЕКТИВНІ НАПРЯМКИ РОЗВИТКУ МЕТОДІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Криптографічні алгоритми є однією з складових частин сучасних систем захисту інформації. Забезпечення криптографічного захисту інформації не можливе без використання довірчих послуг з використанням систем електронно-цифрового підпису (ЕЦП). Тому ЕЦП є основною технологією, від якості і надійності реалізації якої залежить інформаційна безпека держави.

Основним показником безпеки класичних криптографічних алгоритмів є їх криптографічна стійкість (криптостійкість), яка визначається як здатність криптографічного алгоритму протистояти спробам успішного здійснення криптоаналізу з розкриттям або підробленням ключових даних та/або ключової інформації і, як наслідок можливості реалізації загроз порушення конфіденційності, цілісності, справжності, доступності [1]. Цей показник використовується для оцінки безпеки криптосистеми, що не залежить від специфіки її реалізації. Для криптографічних алгоритмів рівень криптостійкості, визначений на момент впровадження, оцінюється в залежності від найефективнішої, відомої на даний момент, атаки, але здатний зменшитися, якщо з часом для алгоритму буде виявлена більш ефективна атака.

Загроза появи та широкого використання квантових обчислювальних систем для класичної криптографії, є принципово новим класом загроз від яких більшість сучасних криптографічних систем, в тому числі системи електронного цифрового підпису, не захищені. Так, за оцінками експертів, наведеними в доповіді NIST про постквантову криптографію [2], до 2030 року стане можливою розробка квантового комп'ютера, здатного зламати криптосистеми за кілька годин.

Сьогодні існує кілька напрямків досліджень постквантових криптоалгоритмів:

криптографія на базі решіток (NTRU), заснована на завданнях решіток з теорії груп - завдання решіток є NP-складними завданнями, рішення яких однаково складне для обчислення як на класичних комп'ютерах, так і на квантових;

багатовимірна криптографія, заснована на рішенні багатовимірних поліномів;

криптографія на основі геш-алгоритмів, заснована на доведеній безпеці хеш-функцій, стійких проти квантових комп'ютерів;

криптографія на основі кодів, представлена криптографічними схемами, заснованими на кодах корекції помилок;

алгоритми обміну ключів з використанням ізогенії суперсінгулярних еліптичних кривих(ЕК).

Алгоритми на основі ізогенії ЕК є цікавим науковим напрямком у зв'язку з можливістю їх полегшеної реалізації на існуючих апаратно-програмних платформах, на яких вже реалізовано скалярне множення точок ЕК. В роботі розглядаються методи криптографічного перетворення підвищеної стійкості до квантового криптоаналізу.

Тому, слід зауважити, що до появи робочих зразків квантових комп'ютерів перехід на нові постквантові алгоритми приведе до зайвих матеріальних витрат. Саме тому необхідно мати методи підвищення криптостійкості алгоритмів ЕЦП на перехідний період.

ЛІТЕРАТУРА:

1. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації /Ю.І.Горбенко за заг. ред. д.т.н., професора І.Д. Горбенка – Харків: Видавництво „Форп”, 2015. – 960 с.

2. Chen L. NISTIR 8105: Report on Post-Quantum Cryptography / L. Chen и др. – NIST, 2016. – 15 с.

ЛАБАРАТОРНИЙ СТЕНД ДЕТЕКТУВАННЯ WIFI ТОЧОК ДОСТУПУ

Актуальність. Зручність бездротових технологій знайоме кожному. Wi-Fi - це популярний термін, що позначає високочастотну бездротову локальну мережу. Технологія Wi-Fi стрімко набирає популярність у багатьох компаніях як альтернатива мережі, побудованої за допомогою кабелів і проводів. Незважаючи на зручність користування технологія Wi-Fi не є стійкою до сучасних кібератак, перехоплення, збору та аналізу трафіку будь-яким користувачем з мінімальними знаннями за допомогою приладів які люди використовують щодня. В зв'язку з чим, метою роботи є розробка лабораторного стенду виявлення Wifi точок доступу з можливістю досліджувати сучасні способи перехоплення трафіку використовуючи різні сучасні сенсори, для виявлення виразливих Wifi точок доступу, аналізу та швидшому їх унунення.

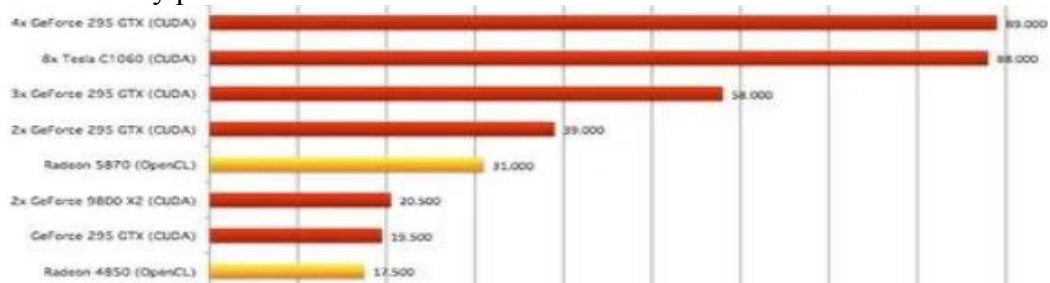
Мета. Метою роботи є створення лабораторного стенду та тестування на вразливості Wifi точок доступу.

Основна частина. Тестування на проникнення бездротового зв'язку вимагає як робочого місця під управлінням Kali Linux і маршрутизатора. Зокрема, для цього тестування ми використовували інструменти Wifite, Reaver, Wireshark, Pmk/s, Aircrack-ng. При тестуванні Wifi маршрутизаторів звертають увагу на 3 пункти такі як : наявність можливості підключення по WPS, наявність вразливості прошивки маршрутизатора та наявність слабкого паролю при створенні закритого ключа WPA/WPA 2 методом грубої сили.

Криптографічно випадковий 8-бітний WPS може надати до 100 мільйонів комбінацій унікальних кодів доступу . Однак WPS насправді відновлення паролю можливе не більше ніж у 11000 припущень. Простота використання цієї вразливості залежить від того, як реалізовано WPS, взлом його проводиться за чотири години, а в деяких випадках він може бути зламаний протягом декількох хвилин.

Що року випускаються в світ сотні варіантів основного коду управління, який вбудований в мережевий пристрій, прошивка маршрутизатора встановлює базовий стандарт безпеки для мережі. Після виявлення вразливості компанії випускають патчі безпеки, які будуть вставлені в останню прошивку для відновлення нещодавно виявлених вразливих місць мережі.

Метод грубої сили— метод рішення криптографічної задачі шляхом перебору всіх можливих варіантів ключа. При цьому, навіть якщо обчислення цільової функції від кожного конкретного можливого рішення задачі може бути здійснена за поліноміальний час, в залежності від кількості всіх можливих рішень повний перебір може зажадати експоненціального часу роботи.



Діаграма 1. Порівняння продуктивності перебору ключів за допомогою сучасних відео-карт методом грубої сили

Висновок. Разом зі стрімким розвитком мережевих технологій, з'являються нові методи пошуку і експлуатування вразливостей, які в руках зловмисників можуть стати причиною витоку конфіденційної інформації, даних про мережу, її топологію та користувачів, що може призвести до подальшого використання цієї інформації в своїх цілях. Ось чому необхідність створення лабораторного стенду потребує розгляду.

ВДОСКОНАЛЕНИЙ МЕТОД АКТИВАЦІЇ ВЕБ-СЕРВІСІВ НА ОСНОВІ БЕЗСЕРВЕРНИХ ХМАРНИХ ОБЧИСЛЕНЬ

Актуальність. Безсерверні обчислення є гарячою темою у світі архітектури програмного забезпечення.

Це поняття вперше було використано для опису програмного забезпечення, яке значною мірою або повністю включає сторонні програми та сервіси, розміщені у хмарі, для керування логікою та станом сервера.

Як правило, це веб-додатки, які використовують велику екосистему доступних у хмарі баз даних, сервісів аутентифікації та інші.

Постачальники хмари пропонують обчислювальні середовища, відомі також як FaaS платформи, де запускається код таких програм.

Назва „безсерверні” використовується тут тому, що рішення по управлінню сервером і плануванню потужностями приховані від розробника або оператора.

Це означає, що вам, як розробнику, не доведеться мати справу з сервером.

Існують очевидні переваги таких програм у порівнянні з традиційними, але у веб-сервісів побудованих за технологією безсерверних обчислень є і недоліки, такі як „холодний старт”, які попри існуючі методи оптимізації все ще залишаються серйозними проблемами ефективності.

Метод активації дозволяє забезпечити паралельність веб-сервісів на основі безсерверних хмарних обчислень.

Ви передаєте програмі скільки екземплярів певного веб-сервісу ви хочете тримати активними і вона впорається з масштабуванням за вас.

Це дозволяє використовувати веб-сервіси з наднизькою затримкою і без „холодного старту”. З часом трафік веб-сервісу може збільшитися, а це означає, що потрібно утримувати більше активних екземплярів, або менше, якщо трафік зменшився.

Потрібно мати деякий коефіцієнт масштабування, який буде автоматично обчислюватись беручи до уваги поточний трафік веб-сервіса.

Це дозволить більш ефективно використовувати веб-сервіси на основі безсерверних хмарних обчислень та зменшити операційні затрати.

Мета. Вдосконалити метод активації веб-сервісів на основі безсерверних хмарних обчислень для підвищення ефективності їх використання.

Основні положення.

Метод активації ґрунтується на асинхронному надсиланні програмою M фіктивних «пінг» запитів до веб-сервіса який потрібно активувати, як показано на рис. 1, тобто мати M активних екземплярів цього веб-сервіса.

Через деякий час бездіяльності веб-сервіса FaaS платформа почне утилізувати активні екземпляри, щоб звільнити хмарні ресурси.

Щоб постійно тримати веб-сервіс активованим потрібно регулярно надсилати M запитів до веб-сервіса.

Значення M та унікальні ідентифікатори веб-сервісів передаються на вхід програмі, яка періодично запускається засобами планувальника.

Значення M вибирається оператором вручну зі статистичних міркувань.

Щоб автоматично обчислювати M потрібно брати до уваги поточний трафік веб-сервіса, що є досить ресурсо-затратним та складно реалізуючим завданням.

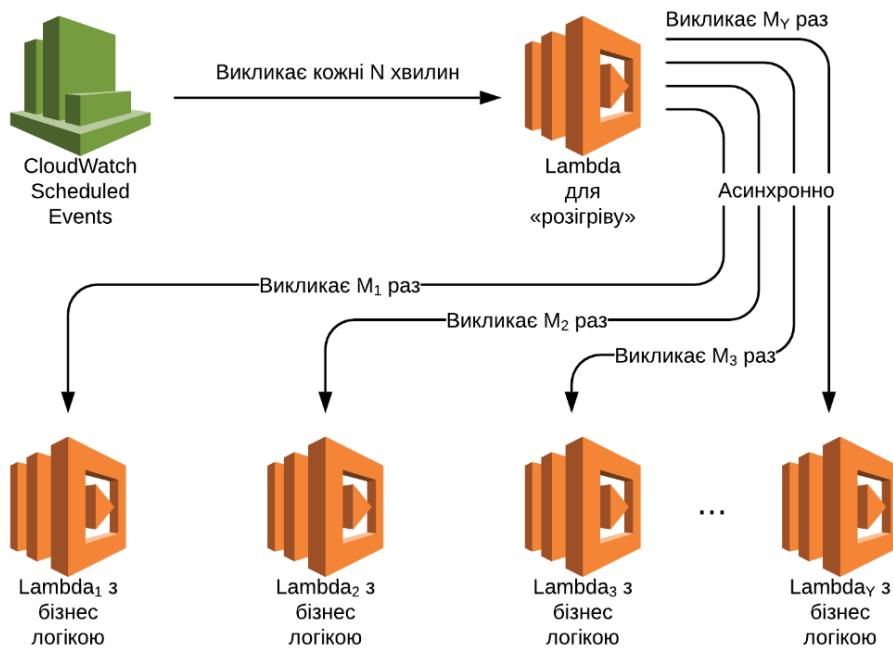


Рис. 1 Високорівнева архітектура методу активації веб-сервісів у інфраструктурі AWS

Скориставшись метрикою використання активних екземплярів веб-сервіса ми можемо робити висновки щодо поточного трафіка цього веб-сервіса. Наприклад, ми хочемо тримати використання активних екземплярів веб-сервіса U близько 70 % (зі статистичних міркувань). Коли поточне використання екземплярів веб-сервіса U' стабільно перевищує 77 % (110% від запланованих 70 %) що відповідає зміні трафіка веб-сервіса за шаблоном вгору, ми можемо збільшити значення M на X , де

$$X = \left(\frac{U' \times 100\%}{U} - M \right)$$

для активації більшої кількості екземплярів, а коли поточне використання U' стабільно менше 63 % (90 % від запланованих 70 %) що відповідає зміні трафіка веб-сервіса за шаблоном вниз, то ми можемо зменшити значення M на X , де

$$X = \left(M - \frac{U' \times 100\%}{U} \right)$$

В результаті нове значення кількості активних екземплярів веб-сервіса M' буде приблизно дорівнювати $M + X$ або $M - X$ відповідно, а поточне значення використання активних екземплярів веб-сервіса U' (яке раніше було $\geq 77\%$ або $\leq 63\%$ відповідно) буде приблизно дорівнювати заданому U (тобто 70 %).

Висновки. На основі проведеного аналізу виявлено проблему низької ефективності використання веб-сервісів на основі безсерверних хмарних обчислень. Аналіз показав, що одним із способів підвищення ефективності використання є вдосконалення методу активації веб-сервісів на основі безсерверних хмарних обчислень. Вдосконаливши метод активації, за рахунок автоматичного обчислення коефіцієнта масштабування активних екземплярів веб-сервіса вдалося підвищити ефективність використання цього веб-сервіса.

МОДИФІКОВАНИЙ СПОСІБ МІЖМАШИННОГО ЗВ'ЯЗКУ ДЛЯ МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ

Згідно концепціям Інтернет Речей і ряду прогнозів в найближчому майбутньому в глобальному масштабі буде проведено декілька телевізійних телекомунікаційних пристроїв. Велика частина цих пристроїв буде так називатися „речами”, що, відповідно до визначення міжнародного союзу електрозв'язку, можуть бути ідентифіковані та інтегровані в мережі зв'язку. M2M є ключем до того, щоб Інтернету речей досягла свого основного бачення, тобто посилення комунікації реальних речей у світі, передачі інформації та виконання розумних завдань. Архітектура мереж бездротових датчиків з низьким енергоспоживанням вважається найбільш підходящою для мереж M2M завдяки своїм низьким витратам і потребам енергії. Бездротові сенсорні мережі зазвичай використовують одну з декількох мережевих топологій для передачі даних.

У топології дерева кластерів множинні кластери зв'язуються один з одним або через голови кластера або маршрутизатори, як показано на рис. 1

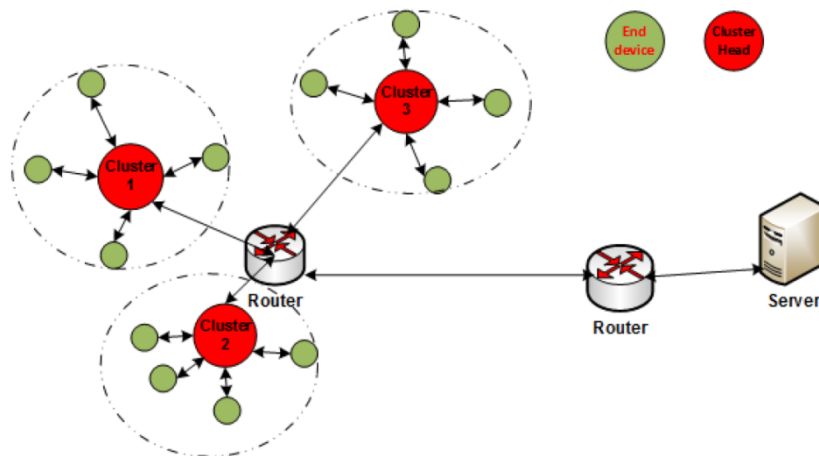


Рис. 1. Мережева архітектура кластерного дерева

Передача даних у сенсорній мережі будується на передачі даних через координатор, який отримує інформацію від кінцевого мережевого пристрою.

Кластеризація є невід'ємною частиною ієрархічних протоколів маршрутизації. У процесі досліджень по кластеризації БСС було розроблено кілька механізмів кластеризації, таких як LEACH, PEGASIS, TEEN і APTEEN. Як правило, ці механізми кластеризації засновані на виборі головного вузла кластера. Тому, найбільш поширеними для кластерних БСС є завдання по розробці алгоритмів вибору головних вузлів кластера.

Поріг визначає мінімальний енергетичний рівень, який повинен мати СН для безпосереднього зв'язку з BS. Тут для простоти розглянуто статичний поріг, що дорівнює половині початкової енергії нормальних вузлів. Але буде більш реалістичним розглянути динамічний поріг, який буде автоматично коригуватися в залежності від середньої залишкової енергії мережі. Якщо залишкова енергія в СН більше порогу, то СН не змінюється. Якщо кластерна головка має меншу енергію, ніж поріг, вона буде замінена відповідно до протоколу LEACH. Запропонований алгоритм (рис.2.)

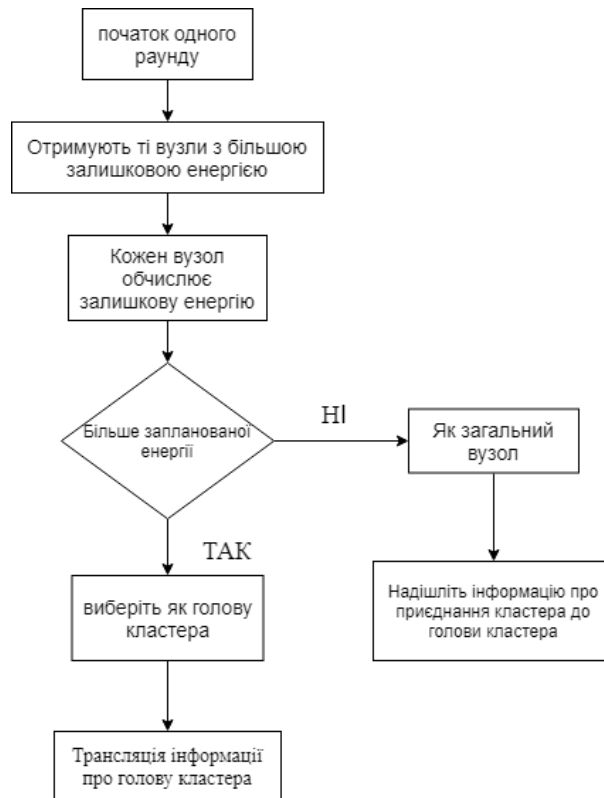


Рис. 2. Алгоритм вибору СН

Виходячи з ідентифікатора і номерів вузлів кластера, графік TDMA (Time Division Multiple Access) буде створений автоматично для присвоєння кожному вузлу часу, коли він може передавати свої дані для кластера. Якщо припустити, що вузол з ним обирається як голова кластера, а вузол з ним призначається перший період для передачі його даних. Один з найважливіших викликів у нашому підході полягає в зменшенні загальної спожитої енергії кожного раунду. Крім того, ми уникаємо споживання енергії через синхронізацію вузлів кластера, коли голова кластера обрана для призначення TDMA. Дійсно, цей спосіб забезпечує відсутність колізій між повідомленнями даних, а також дозволяє радіокомпонентам кожного некластерного вузла відключатися в будь-який час, за винятком часу, коли він виділений для передачі цих даних, що зменшує енергію, споживану вузлами. однак, кластер-голова повинна зберігати свій приймач для того, щоб отримувати дані від інших вузлів. Щоб заощадити більше енергії в бездротовій сенсорній мережі, ми припускаємо, що якщо відстань між вузлом і базовою станцією нижче відстані між цим вузлом і його кластерною головою, то вузол передає свої дані безпосередньо на базову станцію. Також кожен вузол може переміщатися в режимі очікування для зменшення енергоефективності

Висновки: На основі проведеного аналізу виявлені проблеми у мережі Інтернету речей. Аналіз показав, що одним із способів поліпшення мережі є метод кластеризації, за рахунок чого було прийнято рішення поліпшити енергоефективність у мережі методом кластеризації. Запропонований алгоритм було порівняно з ефективністю LEACH та AOVD. Час життя і пропускну здатність нашого запропонованого методу більше, ніж у LEACH і AOVD. Це поліпшення досягається неоднорідністю вузлів і ефективним використанням залишкової енергії кластерних головок, яка залишається невикористаною в LEACH.

МОДЕЛЬ ЗАХИЩЕНОЇ МЕРЕЖЕВОЇ АРХІТЕКТУРИ НА МОБІЛЬНИХ ВУЗЛАХ З ВИКОРИСТАННЯМ ПРОТОКОЛІВ MIP ТА MIPv6

Актуальним напрямком підвищення завадо захищеності сучасних військових мобільних мереж в умовах активної радіоелектронної протидії є застосування всього можливого комплексу та спектру захисту на принципах адаптивного управління. Адаптивне (динамічне) управління ресурсом є одним з найбільш ефективних способів забезпечення заданої якості зв'язку при дії на мережу різних дестабілізуючих факторів. До основних видів ресурсу можна віднести: частотний, енергетичний, просторовий, сигнальний та ін. При цьому, для реалізації адаптивного управління, необхідно передбачити неперервний поточний контроль обстановки, перевірку виконання вимог до якості зв'язку, а також вироблення необхідних управляючих впливів та доведення їх до елементів мережі.

Зазначена вище тема, розглядається з метою побудови моделі мережі, що могла би функціонувати з іншою, порівняно з існуючою, розповсюдженою логікою співвідношення адрес до фізичних пристроїв. Що відповідно могло би вирішити деякі проблеми пов'язані з вразливістю мережевих пристроїв у межах мережевого середовища, що має місце існувати на теперішній час.

У багатьох випадках (наприклад, *VPN*, *VoIP*), раптові зміни в з'єднанні з мережею або *IP*-адрес можуть викликати роз'єднання з мережею. Відповідно при використанні протоколу *Mobile IP*, на якому ґрунтується тема дослідження, що був розроблений для підтримки нерозривного і тривалого підключення до мережевого середовища. *Mobile IP* найчастіше зустрічається в дрітних і бездротових мережах, де користувачам необхідно перенести свої фізичні пристрої через кілька локальних підмереж. Наприклад використання в роумінгу між перекриттям бездротових систем, наприклад *DVB*, *WLAN*, *WiMAX*, і *BWA*.

Область, що розглядається у межах архітектури, ґрунтується на безпечному з'єднанні у межах транспортного рівня, встановленого між мобільною станцією та контролером домашніх станцій, що використовуються, для взаємної автентифікації та завантаження і відповідно, формування загального безпечного з'єднання між елементами мережі. Автентифікація проводиться за допомогою стандартних операцій, де контролером домашніх станцій, використовується сертифікат сервера, для формування своїх облікових даних. Мобільна станція аутентифікує дані та авторизується з контролером домашніх станцій, через повідомлення захищеного з'єднання на транспортному рівні. Будь-який розширюваний протокол автентифікації використовує ключі попереднього доступу автентифікації мобільного агенту до контролерів домашніх агентів. Після успішного завершення автентифікації, контролер домашніх агентів генерує ключі, які отримує вузол. Ця модель безпеки вимагає: щільне з'єднання між частиною протоколу мобільного *IPv6* та *IKE (v2)* / *IPsec* та частин стеку *IP*.

Безпека з'єднання у межах транспортного рівня широко впроваджується майже в усіх основних системах і широко використовується різними додатками. Замість використання *IKEv2*, запропоновані рамками безпеки організовують процес формування повідомлень для обміну ключами і параметрів завантаження між мобільними вузлами. Основною перевагою використання, порівняно із застосуванням *IKEv2*, є простота реалізації і забезпечення еквівалентного рівня безпеки.

КОМБІНАТОРНА M-FSK МОДУЛЯЦІЯ В ДЕКАМЕТРОВОМУ ДІАПАЗОНІ ХВИЛЬ

Постійно зростаючі об'єми в передачі даних спонукають до створення все складнішої, в технологічному плані, апаратури та розробки нових видів сигналів. Крім того, в умовах бойових дій, зокрема поблизу від лінії розмежування та в ході наступальних дій, противником активно застосовується радіоподавлення, що значно ускладнює обмін інформацією. Дана проблема вирішується шляхом застосування складних видів модуляції, однак такий підхід не дозволяє найбільш ефективно використовувати існуючі канали та апаратуру зв'язку. Багатопозиційні квадратурні види модуляції дозволяють значно скоротити час передачі даних проте вимагають високого значення відношення сигнал-шум в каналі зв'язку, крім того високе значення пікфактору даних сигналів ускладнює режим роботи вихідних каскадів передавачів

Одним з найбільш завадостійких видів модуляції є M-FSK (multiple frequency-shift keying), маючи пік фактор вихідного сигналу близький до одиниці даний вид модуляції ефективно задіє можливості вихідного каскаду передавача, однак володіє суттєвим недоліком - швидке зростання ширини спектру вихідного сигналу при збільшенні кількості тонів M . Для прикладу, порівнюючи класичну двох тонову 2-FSK з 16-MFSK маємо восьмикратне збільшення ширини спектру тоді як по швидкості передачі лише чотирикратне. На практиці параметр M обмежують 32, для підвищення швидкості та завадостійкості використовують багатоканальний принцип передачі, що неминуче призводить не лише до збільшення пік фактору сигналу, а й до зменшення відношення сигнал-шум на прийомній стороні.

Для подолання недоліків присутніх M-FSK модуляції пропонується застосування її комбінованої версії, де для передачі одного символу застосовуються не одна частота, а набір з декількох одночасних частот N . Даний підхід дозволяє значно розширити алфавіт можливих символів та зменшити загальну ширину спектра вихідного сигналу. Як приклад, порівнюючи трьох канальну 8-FSK модуляцію, з трьох частотною комбінованою 24-FSK, можна показати збільшення швидкості передачі на 22 % при цьому ширина спектру сигналів і їх пікфактор рівний в обох випадках. В каналах зв'язку, де завадостійкість виходить на перший план комбінована M-FSK модуляція дозволяє підвищити її шляхом застосування меншої кількості одночасно задіяних частот. Застосування комбінаторної M-FSK модуляції дозволяє динамічно змінювати кількість задіяних тонів N , що в свою чергу підвищує швидкість передачі даних та динамічно адаптуватися до умов по завадостійкості. Максимальне, однак не оптимальне, співвідношення досягаються при N , що в двічі менше M .

Принцип формування запропонованого виду модуляції може бути аналогічний ортогональним видам модуляції, в яких ефективно задіяне зворотне перетворення Фур'є. Додавання захисного інтервалу, в кінці кожного символу, додатково підвищить стійкість до між символної інтерференції. Комбінації, що залишилися вільними, доцільно застосувати для символної синхронізації та передачі додаткових службових команд між модемами. Як приклад, у випадку двох частотної комбінованої 24-FSK модуляції, маємо 276 дозволених комбінацій, з яких 256 буде використано для передачі 8-ми бітних символів і 21 лишаються не задіяними.

Як відомо, завадостійкість M-FSK модуляцій, зростає із збільшенням кількості тонів M . Слід очікувати аналогічних показників і для запропонованого виду модуляції. Теоретично було отримано формули для імовірності символної помилки лише для двох частотної M-FSK, інші варіанти можуть бути отримані імітаційним моделюванням. Очікуваний, незначний, програш доцільно компенсувати алгоритмом прямої корекції помилок. Подальші дослідження спрямовані на порівнянні завадостійкості запропонованого виду модуляції з класичними M-FSK та отриманням рекомендацій щодо вибору оптимальних комбінацій частот з набору існуючих, а також співвідношенням між задіяними N та доступними M тонів.

РОЗРОБКА СИСТЕМИ РОЗПІЗНАВАННЯ ЗОБРАЖЕНЬ НА ОСНОВІ АПАРАТУ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ

Актуальність теми доповіді полягає у міцному зв'язку із ситуацією на сході України, а саме: наявність загрози суверенітету та територіальній цілісності держави з боку російського агресора та необхідність застосування модернізованих засобів розвідки, а саме: БПЛА та інших пристроїв з можливістю автоматизованої фото-відео фіксації поля бою та розпізнавання зафіксованих об'єктів, які є потенційними загрозами.

Матеріали доповіді будуть доцільними у використанні під час розробки програмного модуля навчання нейронної мережі та проведення оцінки ефективності програмного модулю. Такий програмний модуль може застосовуватись в ЗСУ для організації автоматизації роботи органів військового управління у сфері розвідки або операторами у об'єктах фото-відео зйомки.

Мета дослідження полягає у проведенні досліджень та аналітичних операцій варіантів розробки систем розпізнавання зображень нейронною мережею зображень за рахунок виконання **наступних завдань**:

- дослідження та аналіз існуючих нейронних мереж розпізнавання зображень та підходів щодо реалізації схем нейронних мереж та методи і можливості їх навчання

- дослідження можливостей та результатів застосування сучасних технологій та засобів автоматизації для роботи органів військового управління у сфері передачі та обробки, основних засобів для розробки системи розпізнавання зображень.

Виклад основного матеріалу. Штучний нейрон – є базовим блоком штучної нейронної мережі. Велика кількість синаптичних зв'язків пов'язують штучні нейрони в одну мережу. Біологічні нейронні мережі з мікроскопічних компонентів існують у тривимірному просторі і здатні до різноманітних з'єднань. Але для реалізації штучних мереж присутні фізичні обмеження. Штучні нейрони можуть утворювати ефективні системи обробки інформації, з'єднуючись у мережі. Вони забезпечують ефективну адаптацію моделі до постійних змін з боку зовнішнього середовища.

В програмній інженерії для проектування ПЗ запропоновані так звані архітектурні шаблони – набір принципів, високорівнева схема, що забезпечує абстрактну інфраструктуру для сімейства систем.

Однією з найважливіших проблем забезпечення якості програмних засобів є формалізація характеристик якості та методологія їх оцінки. Основою регламентування показників якості програмних засобів є міжнародний стандарт *ISO 9126*, яким в основному керуються процеси оцінки якості програмних модулів.

ISO 9126 – це міжнародний стандарт, що визначає оціночні характеристики якості програмного забезпечення. Стандарт поділяється на три частини, що описують наступні питання: модель якості; зовнішні метрики якості; внутрішні метрики якості.

Висновки. Отже, у ході підготовки та викладення матеріалів доповіді виконано дослідження та аналіз загальних відомостей про архітектуру нейронних мереж, основні принципи їх та будови. З'ясовано актуальність обраної теми доповіді та перспективи подальшого застосування викладених матеріалів. Після проведеного аналізу можливостей ШНМ, актуальності її застосування практичної реалізації, на основі результатів виконаних досліджень та з'ясованих та наведених аргументів, можна з впевнено зробити висновки про великий потенціал ШНМ у сучасному світі. Тим паче з урахуванням того, що використання нейронних мереж вже набуло достатнього поширення, в тому числі й у військових цілях (оскільки ваговим плюсом запровадження ШНМ є відсутність вразливого людського фактору).

НОВІТНІЙ ПІДХІД ДО ДІАГНОСТИКИ НЕСПРАВНОСТЕЙ ВИПРЯМНИХ ТРАНСФОРМАТОРІВ ВИСОКОЧАСТОТНИХ ДЖЕРЕЛ ЖИВЛЕННЯ

Актуальність, постановка задачі.

Випрямні трансформатори є ключовими компонентами високочастотних джерел живлення, їх форми хвиль відіграють важливу роль у діагностиці несправностей джерел живлення високої частоти.

Зазвичай в діагностиці несправностей випрямного трансформатора аналізується інтегральне значення поточної форми хвилі.

Однак на форми хвиль струмів суттєво впливають навантаження, що в поєднанні з несправностями призводить до серйозних проблем.

Як правило, звичайні методи не можуть з високою точністю визначити ймовірні несправності, в зв'язку з високими похибками.

Для отримання даних про особливості несправностей пропонується проводити аналіз первинних та вторинних форм хвиль струмів.

Отримані дані передбачається використовувати для навчання векторних машин з підтримкою найменших квадратів щоб створити класифікатори несправностей, таким чином реалізувавши виявлення несправностей та розподіл випрямного трансформатора.

Мета.

Метою доповіді є визначення новітнього підходу до діагностики несправностей випрямних трансформаторів високочастотних джерел живлення.

Основні положення.

У електроенергетиці та інших галузях промисловості широко використовуються високочастотні джерела живлення для електростатичних фільтрів (ESPs). Високочастотне джерело живлення випрямлює трифазну вхідну потужність промислової частоти в постійний струм, який потім перетворюється ланцюгом перетворювача (інвертора) у високочастотний змінний струм на частотах понад 10 кГц.

Після того, як високочастотний трансформатор збільшує напругу і вихідний випрямляч завершує фільтрацію, до частотних джерел електроживлення подається високочастотний пульсаційний струм.

Високочастотне джерело живлення складається з вхідного фільтруючого випрямляча, схеми перетворювача, високочастотного трансформатора та високовольної випрямної схеми. В якості ключового компоненту, продуктивність високочастотного трансформатора безпосередньо впливає на продуктивність всієї системи електропостачання.

Високочастотні трансформатори зазвичай масляні.

Оскільки трансформатор і вихідний випрямляч розміщені в одному занурювальному баку, газ, розчинений у маслі, неможливо виміряти в режимі реального часу.

Отже, підхід на основі трьох співвідношень Міжнародної електротехнічної комісії (ІЕС) 60599, який вимагає точної інформації про розчинений газ і є класичним методом діагностики трансформаторів, не підходить для діагностування цього пристрою. Таким чином, необхідний альтернативний підхід.

Єдиним способом вирішення цієї проблеми є діагностика несправностей за допомогою аналізу форми хвилі.

Для діагностики несправностей випрямного трансформатора в інженерних програмах зазвичай використовуються інтегральні значення первинного і вторинного струму трансформатора.

Однак цей показник не дає достатньої інформації для опису несправностей з'єднання, і це часто призводить до недостовірних результатів діагностики.

Для покращення ефективності діагностики показників високочастотних джерел живлення, потрібен більш ефективний спосіб усунення ознак несправностей.

Отже пропонується вдосконалювати метод діагностики несправностей випрямних трансформаторів високочастотних джерел живлення.

Спочатку необхідно визначити несправність з первинних та вторинних струмів системи за допомогою спеціально розробленого методу визначення характеристик, а потім створити класифікатори векторного апарату підтримки найменшої площі (LS-SVM), використовуючи представлені зразки з різних робочих статусів.

Ці класифікатори використовуються для виявлення та визначення несправностей випрямного трансформатора.

З врахуванням тестового зразку, ці класифікатори LS-SVM можуть ідентифікувати, до якого типу належить зразок, і, таким чином, можна судити про працездатний стан системи.

Основними завданнями новітнього методу є:

підвищення точності діагностики. Оскільки в діагностиці реалізуються нелінійні класифікатори, деякі випадки зв'язку не можуть бути коректно продіагностовані традиційним інтегральним значенням;

спеціально розроблений метод визначення властивостей з поточних форм хвиль. У порівнянні з традиційним методом на основі інтегральних значень, запропонований метод надає набагато більше інформації для діагностики.

Порівняно із загальним методом визначення ознак, таким як розкладання пакетів вейвлетів (WPD) та максимально корельована деконволюція Куртоза (MCKD), запропонований метод легше реалізується і зменшує витрати часу на обчислення результатів.

Висновки.

Таким чином, суттєві переваги запропонованого методу такі:

більш висока діагностична точність, при роботі системи, ніж із застосуванням інтегрального методу, що зазвичай використовується.

більш простий метод вибору для вилучення характеристик з поточних форм хвиль.

У випадках вилучення ознак для поточних форм хвиль, запропонований метод потребує менше часу на обчислення ніж загальні методи вилучення функцій, такі як WPD та MCKD, надаючи при цьому не менше інформації для діагностики. Він також перспективний для діагностики проблеми в критичних ситуаціях, в яких реалізовані форми хвиль для моніторингу стану системи.