МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

ВІЙСЬКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ ІМЕНІ ГЕРОЇВ КРУТ

ВІСНИК ВІТІ

КОМУНІКАЦІЙНІ ТА ІНФОРМАЦІЙНІ СИСТЕМИ

ВИПУСК 1 (4)

Київ
2023

ББК Ц4 (4Укр) 39
З–415

З–415 **Вісник Військового інституту телекомунікацій та інформатизації імені Героїв Крут.** Комунікаційні та інформаційні системи. – Випуск 1 (4). – Київ: ВІТІ, 2023. – 110 с.

Всі наукові статті, викладені у збірнику, прорецензовані фахівцями з відповідних галузей та отримали позитивний відгук.

Збірник затверджено на засіданні Вченої ради інституту (протокол № 11 від 27.08.2023).

ББК Ц4 (4Укр) 39

З М І С Т

УДК 629.3/656

Бригадир С. П. ORCID: 0000-0003-1977-552X (ВІТІ ім. Героїв Крут)
Бондаренко О. Є. ORCID: 0000-0002-9123-7462 (ВІТІ ім. Героїв Крут)
Сергієнко А. В. ORCID: 0000-0001-5336-2089 (ВІТІ ім. Героїв Крут)
Прохорський С. І. ORCID: 0000-0002-6369-2601 (ВІТІ ім. Героїв Крут)

НАУКОВЕ ОБҐРУНТУВАННЯ ТАКТИКО-ТЕХНІЧНИХ ХАРАКТЕРИСТИК КОМПЛЕКСНИХ АПАРАТНИХ ЗВ'ЯЗКУ ТА КІБЕРЗАХИСТУ ДЛЯ ПОТРЕБ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ

Досвід бойового застосування військової техніки зв'язку показує, що вимоги до тактико-технічних характеристик потребують актуалізації не тільки для окремих зразків, але й для цілих сімейств транспортних засобів. Існуючі транспортні засоби для перевезення засобів зв'язку сектору безпеки і оборони базуються на технічно застарілих автомобілях марок ГАЗ, ЗІЛ, КамАЗ, МАЗ, Урал та їхніх модифікаціях, з технічною підтримкою в Росії та Білорусі. Поява кіберзагроз, які потребують захисту інформаційно-комунікаційних вузлів, вимагає створення нових підрозділів у секторі безпеки і оборони. Відповідно, ці підрозділи мали бути оснащені складним обладнанням відповідно до прийнятого модельного ряду. Вітчизняні виробники ПАТ «АвтоКрАЗ» та ТОВ «Трител» виступили з власними ініціативами. Однак відсутність системного підходу та ініціативи створює передумови для вирішення проблеми. Метою цього дослідження є виявлення тактико-технічних характеристик та специфічних вимог до інтегрованих апаратних засобів зв'язку та кібербезпеки майбутнього, тобто переліку автомобільних засобів зв'язку, які відповідатимуть потребам підрозділів сектору безпеки і оборони України. Для досягнення цієї мети в статті проаналізовано сучасний стан публікацій за темою дослідження та виконано часткове завдання демонстрації нових рішень. У статті наведено демонстрацію тактико-технічних характеристик інтегрованих апаратних засобів зв'язку та кіберзахисту для потреб сектору безпеки і оборони України. Отримані результати мають науково-консультативний характер. Остаточне затвердження тактико-технічних характеристик інтегрованих апаратних засобів зв'язку та кібернетичного захисту для потреб сектору безпеки і оборони України залишається на розсуд замовника.

Ключові слова: *комплексний, апаратна, кібернетична безпека, підрозділ, сектор безпеки і оборони.*

S. Brigadier, O. Bondarenko, A. Sergienko, S. Prokhorsky Scientific justification of tactical and technical characteristics of complex hardware communication and cyber protection for security and defense sector needs.

The experience of the combat use of military communication equipment shows that the requirements for tactical and technical characteristics need to be updated not only for individual models, but also for entire families of vehicles. The existing vehicles for the transportation of security and defense sector communications are based on technically obsolete cars of the GAZ, ZIL, KamAZ, MAZ, Ural brands and their modifications, with technical support in Russia and Belarus. The emergence of cyber threats that require the protection of information and communication nodes requires the creation of new units in the security and defense sector. Accordingly, these divisions had to be equipped with complex equipment in accordance with the adopted model range. Domestic manufacturers PJSC "AvtoKrAZ" and LLC "Trytel" came up with their own initiatives. However, the lack of a systematic approach and initiative creates the prerequisites for solving the problem. The purpose of this study is to identify the tactical and technical characteristics and specific requirements for the integrated hardware of communications and cyber security of the future, that is, the list of automotive communications that will meet the needs of units of the security and defense sector of Ukraine. To achieve this goal, the article analyzed the current state of publications on the research topic and performed a partial task of demonstrating new solutions. The article provides a demonstration of the tactical and technical characteristics of integrated communication hardware and cyber defense for the needs of the security and defense sector of Ukraine. The obtained results are of a scientific and advisory nature. The final approval of the tactical and technical characteristics of the integrated hardware means of communication and cyber protection for the needs of the security and defense sector of Ukraine remains at the discretion of the customer.

Keywords: *complex, hardware, cyber security, subdivision, security and defense sector.*

Постановка проблеми. Існуючий досвід бойового застосування військової техніки підрозділами сектору безпеки і оборони в антитерористичної операції, операції Об'єднаних сил та війні свідчить про необхідність актуалізації вимог до тактико-технічних характеристик (ТТХ) окремих зразків техніки [1]. З появою нових підрозділів Військ зв'язку та кібербезпеки безумовно з'явилась зацікавленість в нових зразках техніки для забезпечення їхніх потреб [2; 3].

На сьогодні автопарк сектору безпеки і оборони України базується на технічно застарілих автомобілях ГАЗ, ЗІЛ, КамАЗ, КрАЗ, МАЗ, Урал та їхніх модифікаціях [4]. Ремонтні комплекти для всіх типів транспортних засобів, окрім КрАЗів, доступні лише в країні-окупанта та її союзника.

Деякі вітчизняні виробники, в тому числі КрАЗ, вже активно розробляють та пропонують власні рішення та зразки різних конструкцій з різними характеристиками та експлуатаційними показниками на базі базових шасі вітчизняного та іноземного виробництва для задоволення потреб сектору безпеки і оборони України (ПАТ «АвтоКрАЗ» [5], ТОВ «Трител» [6] та ін.).

Аналіз останніх досліджень і публікацій. Проаналізовано в [7] технічні характеристики бронеавтомобілів Збройних сил України виробництва ПАТ «АвтоКрАЗ». Зроблено висновок про доцільність продовження модернізації машин. Аналогічні думки були висловлені і щодо заміни старої техніки на нове озброєння [4].

Закупівля автомобільної техніки іноземного виробництва під час повномасштабної війни накладає на державу фінансові зобов'язання на додаткові потреби, пов'язані з експлуатацією, обслуговуванням, постачанням запасних частин та/або розвитком інфраструктури та ремонтних потужностей для відновлення збройних сил [8].

Слід зазначити, що автори робіт [9–12] вже визначили певні системні обриси перспективних сімейств автомобільної бази, які повністю відповідають сучасним вимогам сектору безпеки і оборони України.

Виділення аспектів, що недостатньо вивчені. Так, існує необхідність розробки комплексної апаратної зв'язку та кібернетичного захисту (КАЗ), що відповідає потребам підрозділів сектору безпеки і оборони України на основі уніфікованого шляху із замкнутим технологічним циклом виробництва. Тактико-технічні характеристики КАЗ повинні забезпечувати виконання завдань, покладених на сектор безпеки і оборони України відповідно до сучасних оперативно-тактичних вимог та функціональних завдань.

Метою цієї статті є наукове обґрунтування для КАЗ, необхідних для сектору безпеки і оборони України.

Виклад основного матеріалу.

Метою створення КАЗ є організація мобільного комплексу завдань для швидкого та зручного підключення технічних систем моніторингу стану кібербезпеки вузлів зв'язку різних рівнів управління.

Для реалізації мобільного функціоналу комплексу кібербезпеки необхідно розробити технічні завдання на інструментальну базу та комплектуючі, виробників з повним замкнутим циклом виробництва [12].

На думку [2; 3] КАЗ має забезпечити виконання наступних завдань:

розміщення універсального комплекту обладнання для комплексного кібернетичного контролю та захисту вузлів зв'язку відповідного призначення;

швидке пересування на великі відстані різними дорогами та ґрунтами;

забезпечення працездатності та побуту особового складу на заставі;

забезпечення цілодобового чергування на посту вузла зв'язку відповідно до функціональних завдань;

забезпечення життєдіяльності та відпочинку персоналу.

Виходячи з цих вимог, ескізний проєкт КАЗ складається з двох компонентів: зони для організації 24-годинної зміни та зони відпочинку.

Необхідно розробити модернізовані технічні характеристики та вимоги до умов експлуатації КАЗ та його обладнання:

обладнання повинно працювати у повній відповідності до технічних умов під впливом механічних та кліматичних факторів, спеціальних середовищ та іонізуючого випромінювання з космосу, при температурі навколишнього середовища від –50 ˚С до +50 ˚С, вологості 0–95 % та атмосферному тиску 700–800 мм рт. ст.;

необхідний захист від ураження блискавкою, електромагнітними полями грозових розрядів, електростатичними розрядами, що накопичуються в промислових електромережах, електричними полями, що створюються лініями електропередачі, апаратурою та іншими пристроями, а також іншими радіоелектронними засобами;

захист екіпажу від впливу ядерної, хімічної та біологічної зброї, а також зовнішніх природних факторів ураження;

броньований захист машин, екіпажу та обладнання від куль калібру до 7,62 мм, мін та саморобних вибухових пристроїв;

обладнання монтується в стандартну 19-дюймову серверну шафу в стійку, 6-дюймову шафу в стійку та додаткову стійку або стіл;

робоча напруга джерела живлення повинна становити 180–240 В, а резервна потужність електроустановки – не менше ніж 5000 Вт;

заземлення обладнання відповідно до вимог ГОСТ 16556-81;

кондиціонери кузова повинні забезпечувати відсутність надлишкового тиску повітря всередині під час роботи штатної системи фільтровентиляції;

системи пожежної сигналізації та визначені місця розташування вогнегасників;

заземлення обладнання та установок – передбачити контур заземлення, припаяний і приєднаний до клем заземлення обладнання, блоків і панелей;

працездатність забезпечується в дорожніх і ґрунтових умовах, визначених для шасі, на допустимих швидкостях відповідно до умов безпеки і допустимих швидкостях при подоланні природних і штучних перешкод, під час і після впливу механічних факторів, що виникають при русі відсіку обладнання власним ходом дорогами і бездоріжжям, і відповідно до функціональних завдань повинна працювати;

обладнання, встановлене поза кузовом транспортного засобу, повинно працювати при температурі навколишнього середовища від –50 °С до +50 °С та під впливом атмосферних опадів (дощ, іній, роса).

Склад обладнання КАЗ. Виходячи з функціональних завдань, покладених на КАЗ, пропонується орієнтовний набір телекомунікаційного обладнання і засобів зв’язку та кіберзахисту за аналогією зі зразком [10], який наведено в таблицях 1–4.

Враховуючи телекомунікаційне обладнання та засоби зв’язку КАЗ, слід обрати вантажний автомобіль великої вантажопідйомності. Значний вітчизняний виробничий потенціал із замкнутим технічним циклом з виробництва автомобілів підвищеної прохідності наведено в [12], ПАТ «АвтоКрАЗ» відповідає цій вимогі. Перелік продукції для військового сектору доступний на офіційному сайті [6]; висока прохідність, надійність та ремонтопридатність автомобілів КрАЗ гарантують їх масове використання для виконання широкого спектру спеціальних завдань [12]. Орієнтовний перелік апаратного оснащення наведено в таблиці 1.

Таблиця 1

Орієнтовний перелік апаратного оснащення

Найменування обладнання і засобів зв’язку	***Орієнтовна комплектація***	
	Тип	***К-сть (шт.), не менше***
Апаратне обладнання:		
Телекомунікаційний комплект. Засоби КХ-радіозв’язку	ТК-2 HARRIS Falcon II (III)	2 1
Засоби УКХ-радіозв’язку (мобільний/автомобільний). Ретранслятор УКХ-радіозв’язку (транкінговий)	Motorola Motorola	4/1 1
Комплект станцій (терміналів) супутникового зв’язку	Tooway	1
Комплект станцій (терміналів) супутникового зв’язку. Засоби (вироби) криптографічного шифрування	Starlink	1 1

Найменування обладнання і засобів зв'язку	*Орієнтовна комплектація*	
	Тип	*К-сть (шт.), не менше*
VoIP-шлюзи (16 портів)		2
Телефонні апарати	Panasonic	16 + 16 + 4
Захищений ноутбук	Panasonic	4
МФУ (принтер, сканер, ксерокс для службових потреб). Безперебійний блок живлення	МФУ 5 кВт	1 2
Радіосканер (R&S®FPH Spectrum Analyzer Instrument Security Procedures)	Rohde & Schwarz	1
Комутатор некерований. Комутатор некерований PoE (4 порти)	 TP-LINK / ZyXEL	2 1

У таблиці 2 представлено орієнтовний перелік антено-фідерного та кабельного майна.

Таблиця 2

Орієнтовний перелік антено-фідерного та кабельного майна

Найменування антено-фідерного та кабельного майна	*Орієнтовна комплектація*	
	Тип	*К-сть (шт.), не менше*
Антено-фідерне обладнання:		
Антена КХ діапазону	Harris Falcon II (III)	1
Антена УКХ діапазону (автомобільний варіант) колінеарний / направлена	Motorola	1/1
Кабельне майно:		
Вита пара	F/FTP, S/FTP, SF/FTP	2000 м
Кабель польовий	П-274	1000 м

Визначимо технічні характеристики КАЗ на базі автомобіля.
Електрична система автомобіля подає до споживача напругу 12 В або 24 В.
Вимоги до бронезахисту автомобіля та КУНГ такі:
автомат АК-74 (куля 5,45 мм);
автомат АКМ (куля 7,62 мм);
гвинтівка СВД (куля 7,62 мм);
міни, саморобні вибухові пристрої.
У таблиці 3 викладено приблизний перелік програмного забезпечення.

Таблиця 3

Приблизний перелік програмного забезпечення

Найменування програмного забезпечення	*Орієнтовна комплектація*	
	Тип	*К-сть (шт.), не менше*
Програмне забезпечення:		
Install антивірусне програмне забезпечення (АВПЗ)	ПЗ	4
Програма диспетчер для радіозасобів	СПЗ	комплект
Програмне забезпечення програмування радіозасобів (до кожного типу засобів)	СПЗ	комплект
USB-накопичувач install Windows (XP/Vista/7/8/10/11)	ПЗ	комплект
Install Microsoft Office (Word/Excel/PowerPaint/Visio) Office 2013/2016	ПЗ	комплект
Поштовий клієнт для операційних систем Microsoft Windows	ПЗ	комплект
Програмне забезпечення «карта висот»	ГІС «Карта 2011»	1
Програмне забезпечення навігації		1 (2)

У таблиці 4 викладено приблизний перелік допоміжного обладнання.

Таблиця 4

Приблизний перелік допоміжного обладнання

Найменування допоміжного радіотехнічного майна	***Орієнтовна комплектація***	
	Тип	***К-сть (шт.), не менше***
Допоміжне радіотехнічне майно:		
Пристрій нічного бачення		1
Камери зовнішнього відеоспостереження		3
Навігатор		1
Шуруповерт електричний (акумуляторний)		1
Тестер для вимірювання параметрів Ethernet		1
Генератор тональних сигналів для перевірки кабельних ліній (тестер мережі RJ-45, RJ-12 з генератором тону)		1
Подовжувач з розеткою	Довжиною 50–100 м	2
Подовжувач з розетками	Довжиною до 5 м	4
Електричний паяльник	12/220 В	1

У таблиці 5 викладено вимоги до технічних характеристик автомобільної бази КАЗ.

Таблиця 5

Вимоги до технічних характеристик автомобільної бази КАЗ

№ з/п	***Найменування технічної характеристики***	***Значення, не гірше***
1.	Колісна формула	4×4
2.	Повна маса	25 150 кг
3.	Двигун	Дизельний
4.	Робочий об’єм	14,85 л
5.	Потужність двигуна	300–400 к. с.
6.	Максимальний крутний момент	1521 Н*м
7.	Коробка передач	механічна
8.	Кількість швидкостей	8 + 1
9.	Максимальна швидкість пересування, км/год	90
10.	Максимальний кут подолання підйому, град	35
11.	Контрольна витрата палива, л/100 км	Не більше 35
12.	Мінімальний радіус повороту, м	13
13.	Дорожній просвіт при повному завантаження, мм	400
14.	Шини	530/75-R21 (1300×3–533)
15.	Ємність паливних баків, л	2×250
16.	Балістичний захист за ДСТУ 3975	ПЗСА-4
17.	Екіпаж, чол.	До 6

Наразі існують різні типи рішень щодо габаритів КУНГ (рис. 1).

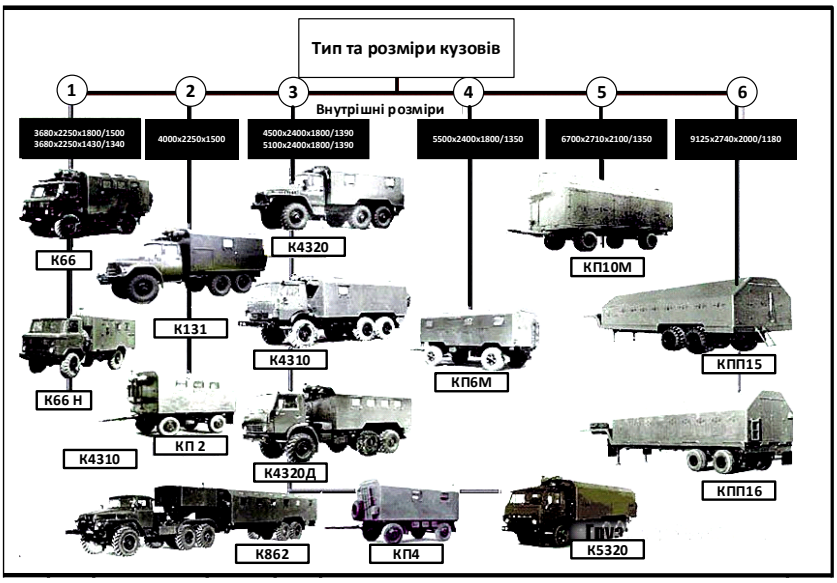

Рис. 1. Типи та габарити кузовів

Досвід з бойового застосування дослідних зразків КАЗ на базі КрАЗ, Урал, ЗІЛ та КамАЗ в антитерористичних операціях, спільних військових операціях та бойовому застосуванні під час війни дозволив визначити оптимальні вимоги до КУНГ КАЗ (табл. 6).

У таблиці 6 вказано технічні характеристики КУНГ.

Таблиця 6

Технічні характеристики КУНГ

№ з/п	*Найменування технічної характеристики*	*Значення, не гірше*
1.	Габаритна довжина, мм	8 550
2.	Габаритна ширина, мм	2 700
3.	Габаритна висота, мм	3 600

КУНГ КАЗ монтується на шасі автомобіля (виробу) і призначена для перевезення, транспортування та експлуатації спеціалізованого обладнання.

Автомобільний КУНГ закритого типу без каркасної конструкції з панелей армованого пінопласту, оснащений системою опалення та вентиляції, системою освітлення для його експлуатації.

Можливість працювати 24 години на добу в різних кліматичних умовах і температурі навколишнього середовища від –40 °С до +50 °С.

Для забезпечення комфортних умов роботи особового складу та належного функціонування обладнання і приладів як у мирний час, так і під час бойових дій, кузовні фургони повинні бути обладнані дизельною системою опалення та вентиляції ОВ-65 та фільтровентиляційною системою ФВУА-100Н-12, яка знезаражує повітря, що подається в кузов транспортного засобу, шляхом створення надлишкового тиску.

Для забезпечення харчування особового складу в польових умовах або в автономному режимі роботи КАЗ повинен бути передбачений харчоблок (табл. 7).

Таблиця 7

Орієнтовний перелік комплекту харчоблока

Найменування майна	***Орієнтовна комплектація***	
	Тип	***К-сть (шт.), не менше***
Чайник	Електричний (800–1200 Вт)	1
Чайник	Металевий	1
Казан	Металевий	1
Мікрохвильова плита	800–1200 Вт	1
Електрична плита	800–1200 Вт	1
Тринога	Металева	1
Набір столового посуду на 4 персони	Металевий	1
Решітка-гриль	Металева	1

Крім того, майбутні КАЗ повинні бути оснащені додатковими інженерно-технічними та економічними засобами (табл. 8).

Таблиця 8

Орієнтовний перелік додаткових інженерно-технічних та економічних засобів

Найменування майна	***Орієнтовна комплектація***	
	Тип	***К-сть (шт.), не менше***
Інженерне майно:		
Паяльна лампа, 2л Т-40М	Мотор Січ	1
Бензопила (електропила)		1
Сокира		1
Клин		1
Маскувальна сітка		1
Велика саперна лопатка	БСЛ-110	2
Каністра для ПММ	20 л	2
Лійка		1
Груша (ПММ)		1
Господарське майно:		
Рукомийник (10 л)		1
Віник		1
Відро		1
Щітка		1
Віpьовка		1
Ємність для питної води не менше 10 л		2
Палатка на 4 особи		1

Вимоги щодо підвищення живучості завдяки використанню підвісних багатосекційних паливних баків [10]. Проєктовані паливні баки повинні бути обладнані багатошаровою зовнішньою оболонкою (захисною оболонкою), яка зміцнює стінки бака і запобігає витоку палива при механічних пошкодженнях. Захисна оболонка повинна містити еластичний матеріал, який розширюється під впливом пального і закриває отвори, що утворюються в разі механічного пошкодження бака.

Весь об’єм паливного бака повинен бути заповнений газопроникним наповнювачем для утримання вибухонебезпечної пароповітряної суміші і запобігання раптового займання, що викликає підвищення тиску, яке може призвести до руйнування бака.

Висновки. Отже, враховуючи розглянуті технічні характеристики та вимоги до виробництва КАЗ, доцільним є використання можливостей українського автомобільного заводу ПАТ «АвтоКрАЗ». При цьому буде забезпечено раціональне використання коштів державного оборонного бюджету, спрямованих на виробництво та ремонт КАЗів вітчизняними підприємствами.

Очікується, що створення КАЗ та оснащення ними підрозділів сектору безпеки і оборони підвищить рівень оперативної готовності підрозділів і дозволить їм виконувати спеціальні завдання у сферах боєздатності та кібербезпеки.

Подальші дослідження мають бути зосереджені на розробці технічних специфікацій для КАЗ на базі транспортних засобів, що пересуваються на високій швидкості дорогами з твердим покриттям.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кривошеєв В. В., Кацалап В. О. Аналіз експлуатації діючих макетів комплексу спеціальних апаратних для підрозділів інформаційно-психологічних операцій // Сучасні інформаційні технології у сфері безпеки та оборони. 2020. № 1 (37). С. 197–202.

2. Воронков С. Генерал-майор Євген Степаненко: «Головне завдання – привести систему зв'язку нашого війська до стандартів НАТО» // АрміяINFO. URL: https://armyinform.com.ua/2020/08/07/general-major-yevgen-stepanenko-golovne-zavdannya-pryvesty-systemu-zvyazku-nashogo-vijska-do-standartiv-nato.

3. Розвиток та потенційні можливості командування військ зв'язку та кібербезпеки // Армія FM. URL: https://www.armyfm.com.ua/rozvitok-ta-potencijni-mozhlivosti-komanduvannya-vijsk-zv'yazku-ta-kiberbezpeki-/.

4. Мусієнко В. А., Гришина Н. С., Савченко О. М., Івченко М. М., Ткач В. О. Аналіз існуючих апаратних технічного забезпечення засобів зв'язку і АСУВ та підходи щодо розробки таких апаратних тактичної і оперативно-тактичної ланок управління // Збірник наукових праць ВІТІ. 2017. № 4. С. 76–83.

5. Каталог автомобілів КрАЗ // Компанія «АвтоКрАЗ»: офіційний сайт. URL: http://www.autokraz.com.ua/downloads/catalogue.pdf.

6. Комплексна апаратна зв'язку // ТОВ «Трител». URL: http://www.tritel.ua/index.php/uk/produktsiya/spetsialnye-sredstva-svyazi/kompleksnaya-apparatnaya-svyazi/kompleksnaya-apparatnaya-svyazi-detail.

7. Дунь С. В., Кайдалов Р. О. Розвиток модельного ряду броньованих автомобілів КрАЗ // Перспективи розвитку озброєння та військової техніки Сухопутних військ: збірник тез доповідей Міжнародної. наук.-техн. конф. Львів: АСВ, 2015. С. 30.

8. Костюк В. В., Русіло П. О., Варванець Ю. В., Калінін О. М. Основні критерії щодо створення перспективного сімейства вітчизняних бойових колісних машин // Системи озброєння і військова техніка. 2016. № 1 (45). С. 25–28.

9. Грубель М. Г., Козлов Д. В., Козлинський М. П. Формування основних параметрів типажу військової автомобільної техніки // Проблеми координації воєнно-технічної та оборонно-промислової політики в Україні. Перспективи розвитку озброєння та військової техніки: матеріали VI Міжнародної науково-практичної конференції, м. Київ, 11–12 жовтня 2018 р. Київ: ЦНДІ ОВТ ЗС України, 2018. С. 87.

10. Шемендюк О. В., Козубцов І. М., Нещерет І. Г., Процюк Ю. О., Бригадир С. П., Фомкін Д. В. Обрис функціонального призначення, потреб у складі обладнання і засобів комплексної апаратної зв'язку та кібербезпеки // Кібербезпека: освіта, наука, техніка. 2022. Том 2. № 18. С. 61–72.

11. Шаповал В. В., Радзівілов Г. Д., Османов Р. Н., Сердюк П. Є. Роль і місце сучасних бронеавтомобілів в українських військових формуваннях // Вісник ВІТІ. Комунікаційні та інформаційні системи. 2021. № 2. С. 108–113.

12. Козубцов І. М., Куцаєв В. В., Козубцова Л. М., Терещенко Т. П., Штонда Р. М, Черноног О. О. Обґрунтування вибору автомобільної платформи для підрозділів кібернетичної безпеки Збройних Сил // Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку: матеріали Міжнародної науково-практичної конференції, м. Харків, 15 березня 2019 р. Харків: Національна академія Національної гвардії України, 2019. С.55–57.

УДК 621.391

Івченко М. М. ORCID: 0000-0002-0039-2812 (ВІТІ ім. Героїв Крут)
Білий О. А. ORCID: 0000-0003-3056-8562 (ВІТІ ім. Героїв Крут)
Атаманенко М. В. ORCID: 0000-0001-5381-0224 (ВІТІ ім. Героїв Крут)
Карабань О. В. ORCID: 0000-0002-5286-7373 (ВІТІ ім. Героїв Крут)
Шугалій О. О. ORCID: 0000-0002-6587-0096 (ВІТІ ім. Героїв Крут)
Цимбал І. В. ORCID: 0000-0002-5286-7373 (ВІТІ ім. Героїв Крут)

АНАЛІЗ ЕФЕКТИВНОСТІ ОРГАНІЗАЦІЇ ТЕХНІЧНОГО ТА СЕРВІСНОГО ЗАБЕЗПЕЧЕННЯ ТЕХНІКИ ЗВ'ЯЗКУ І ЗАСОБІВ АВТОМАТИЗАЦІЇ В ЗБРОЙНИХ СИЛАХ УКРАЇНИ

У сучасному світі, де технології відіграють ключову роль у веденні війни, ефективне використання та обслуговування систем військового зв'язку є важливим елементом оборонної стратегії. Дослідження факторів, що впливають на ефективність використання цих систем в Збройних силах України, є актуальним та важливим завданням.

Організація технічного та сервісного забезпечення техніки зв'язку і засобів автоматизації є важливою складовою діяльності будь-яких військових формувань, включаючи Об'єднані збройні сили НАТО. Ефективне функціонування та органічне поєднання цих складових є критичним для успішного виконання військових операцій.

Ця наукова стаття присвячена аналізу ефективності організації технічного та сервісного забезпечення техніки зв'язку і засобів автоматизації в Збройних силах України в контексті сучасних військових операцій, швидкого розвитку технологій та зростанні складності бойових завдань, ефективного функціонування комунікаційних систем та автоматизованих комплексів, має вирішальне значення для забезпечення безпеки та успішності військових операцій. У цій статті розглянуто основні напрямки, які вимагають уваги та відповідних інвестицій у галузі технічного та сервісного забезпечення зв'язку і автоматизації у Збройних силах України.

Загалом, аналіз ефективності технічного та сервісного забезпечення техніки зв'язку і засобів автоматизації в Збройних силах НАТО вимагає комплексного підходу та врахування багатьох факторів.

Під час проведення досліджень військових операцій та аналізу досвіду застосування Збройних сил України можемо виділити один з найважливіших факторів – це упровадження системи управління життєвим циклом техніки зв'язку і засобів автоматизації, на кшталт використання таких систем у Об'єднаних збройних силах НАТО та створення новітньої системи технічного обслуговування та ремонту техніки зв'язку і засобів автоматизації.

Ключові слова: *упровадження системи управління життєвим циклом, технічне та сервісне забезпечення техніки зв'язку і засобів автоматизації, система технічного обслуговування та ремонту, стандарти НАТО, діаграма Ішикави.*

M. Ivchenko, O. Bilyi, M. Atamanenko, O. Karaban, O. Shuhalii, I. Tsymbal Analysis of the effectiveness of the organisation of technical and service support for communications and automation equipment in the Armed Forces of Ukraine.

In today's world, where technology plays a key role in warfare, the effective use and maintenance of military communications systems is an important element of defense strategy. Researching the factors that influence the efficiency of these systems in the Armed Forces of Ukraine is a relevant and important task.

The organization of technical and service support for communications and automation equipment is an important component of the activities of any military formations, including the NATO Allied Forces. The effective functioning and organic combination of these components is critical for the successful execution of military operations.

This scientific article is devoted to the analysis of the effectiveness of the organization of technical and service support for communications equipment and automation in the Armed Forces of Ukraine in the context of modern military operations, rapid development of technologies and increasing complexity of combat missions, the effective functioning of communication systems and automated systems is crucial for ensuring the safety and success of military operations. This article discusses the main areas that require attention and appropriate investments in the field of technical and service support of communications and automation in the Armed Forces of Ukraine.

In general, the analysis of the effectiveness of technical and service support for communications and automation equipment in the NATO Armed Forces requires a comprehensive approach and consideration of many factors.

In the course of researching military operations and analysing the experience of the Armed Forces of Ukraine, we can identify one of the most important factors is the introduction of a life cycle management system for communications and automation equipment, such as the use of such systems in the NATO Allied Forces and the creation of a modern system for the maintenance and repair of communications and automation equipment.

Keywords: *implementation of a life cycle management system, technical and service support of communication and automation equipment, maintenance and repair system, NATO standards, Ishikawa diagram.*

Постановка завдання в загальному вигляді

Сучасні бойові умови вимагають від Збройних сил України ефективної комунікаційної системи та автоматизованих комплексів, які забезпечують надійне функціонування, координацію та інформаційну взаємодію між різними рівнями командування. Оскільки сучасні військові операції відбуваються в умовах швидкої зміни ситуації та викликають великі навантаження на комунікаційні системи, важливо розглянути пріоритетні напрямки розвитку технічного та сервісного забезпечення зв'язку і засобів автоматизації в Збройних силах України.

Досвід застосування підрозділів при веденні операцій в умовах повномасштабної війни, розв'язаної російською федерацією, показує, що однією з актуальних проблем є належне забезпечення технічного обслуговування та ремонту всіх наявних видів техніки зв'язку і засобів автоматизації (далі – ТЗА) під час виконання ними завдань за призначенням.

Організація технічного та сервісного забезпечення ТЗА є важливою складовою діяльності будь-яких військових формувань, включно зі Збройними силами НАТО. Ефективне функціонування технічного та сервісного забезпечення є критичним для успішного виконання військових операцій.

Для аналізу ефективності такої організації можна використовувати різні підходи та методики. Один із можливих підходів – це аналіз факторів, які впливають на ефективність організації технічного та сервісного забезпечення ТЗА з використання діаграми Ішикави та аналізу передових практик, які застосовуються в Об'єднаних збройних силах (далі – ОЗС) країн-членів НАТО. Це дозволяє виявити сильні та слабкі сторони системи порівняно з іншими.

Також важливим елементом аналізу є **оцінка стану технічного забезпечення**, яка містить оцінку наявності сучасної техніки, рівня її готовності до використання при веденні бойових дій, наявності та ефективності функціонування систем підтримки та обслуговування.

Для **оцінки ефективності сервісного забезпечення** можна вивчити такі параметри, як час відновлення обладнання після відмови, використання резервних систем, наявність та якість запасного майна та приладдя, радіоелектронних компонентів, рівень підготовки висококваліфікованих фахівців ремонтників, а також швидкість виконання ремонтно-відновлювальних робіт та проведення технічного обслуговування.

Загалом, аналіз ефективності технічного та сервісного забезпечення ТЗА в ОЗС НАТО вимагає комплексного підходу та врахування багатьох факторів. Він може бути виконаний експертами з соціальних, технічних та стратегічних наук, які вивчають проведення військових операцій та досвід застосування Збройних сил України.

Проаналізувавши вимоги основних керівних документів, які мають посилання щодо основних напрямків розвитку та завдань технічного та сервісного забезпечення ТЗА в Збройних силах України [1–6], слід зазначити, що пріоритетним напрямом це є «розвиток за стандартами НАТО системи логістичного забезпечення Збройних сил України та інших складових сил оборони під час виконання завдань всеохоплюючої оборони України, автоматизація логістичних процесів, їх об'єднання з відповідними процесами національної економіки для підтримки операцій Об'єднаних сил» [1; 5].

Аналіз останніх досліджень і публікацій

Аналіз досліджень організації технічного та сервісного забезпечення ТЗА в Збройних силах України, які запропоновані (реалізовані) в Україні та збройних силах провідних країн світу, відображено в роботах [7–12].

Під час проведення цих досліджень на основі аналізу військових операцій та досвіду застосування сил оборони держави можемо виділити один із найважливіших факторів організації технічного та сервісного забезпечення ТЗА в Збройних силах України, – це упровадження системи управління життєвим циклом техніки зв'язку і засобів автоматизації

на кшталт використання таких систем у ОЗС НАТО та створення новітньої системи технічного обслуговування та ремонту (далі – ТОР) ТЗА.

Зважаючи на те, що більша частини ТЗА є іноземного виробництва і позбавлена авторського нагляду, в Україні була розроблена низка нормативно-правових актів, які дозволили унормувати діяльність щодо відновлення, ремонту, модернізації, збільшення установленого ресурсу та продовження строку служби (зберігання) озброєння, військової і спеціальної техніки, за якими не здійснюється авторський нагляд [3].

Водночас авторами [8] визначені проблемні питання, які стримують процес переходу на сучасні методи експлуатації озброєння та військової техніки, а саме: низькі темпи впровадження нормативної, науково-методичної й економічної бази, засобів контролю граничного (технічного) стану, діагностичних засобів. Крім того, в [12] зазначено, що зниження експлуатаційних і ремонтних витрат при переведенні й експлуатації за технічним станом повинно забезпечуватися: заміною трудомістких і високовартісних регламентованих заводських (середніх і капітальних) ремонтів комплексів – контролем граничного стану, відновлювальними роботами, військовим ремонтом за результатами контролів граничного стану, ремонтами за технічним станом; зниженням трудомісткості ТОР за рахунок впровадження методів технічної експлуатації за станом, формуванням раціональних режимів ТОР, бригадних та інших централізованих форм їх виконання; скороченням кількості запасних частин у зв’язку з відміною призначених термінів служби і ресурсів (і відповідних планових замін і ремонтів). У роботі [13] проаналізовано стратегії ТОР, які використовуються в Військово-повітряних силах США, за результатами чого визначено, що стратегія ТОР за наробітком застосовується для 6–10 % виробів, стратегія з контролем параметрів – для 15–31 %, з контролем рівня надійності – для 63–75 %, оскільки вона найбільш відповідає вимогам експлуатації в умовах бойового застосування.

Аналіз показав, що питанням відповідності нині діючої у Збройних силах України системи технічного обслуговування та ремонту ТЗА, обґрунтуванню шляхів та методів її удосконалення, з урахуванням вимог керівних документів та з урахуванням нині діючих підходів, які прийняті в ОЗС НАТО до технічного обслуговування, враховуючи те, що на постачання підрозділів та частин Збройних сил України надходить ТЗА на новій елементній базі, – висвітлено недостатньо, а керівні документи з питань технічного обслуговування та ремонту ТЗА застарілі і потребують внесення змін, доповнень, а можливо і переопрацювання їх в повному обсязі. Тому дослідження визначених завдань дозволить розглянути та прийняти до виконання нову систему ТОР ТЗА в Збройних силах України, а в майбутньому і використати ці дослідження при переопрацюванні керівних документів із технічного та сервісного забезпечення ТЗА в цілому.

Нині вже проведено ряд досліджень та публікацій щодо організації технічного та сервісного забезпечення ТЗА як в країнах, що входять до складу ОЗС НАТО, так і підходів до цих систем в Збройних силах розвинених країн світу, але в них, на наш погляд, одночасно повинно бути досліджено також і питання з підготовки фахівців ремонтників ТЗА, щоб у майбутньому запропонувати перспективну систему ТОР ТЗА, забезпечити підготовку фахівців ремонтників в Збройних силах України, яка б відповідала існуючій системі, яка прийнята в ОЗС НАТО.

Мета статті полягає в проведенні як аналізу організації технічного та сервісного забезпечення ТЗА в Збройних силах України, так і аналізу досвіду з підготовки фахівців ремонтників в країнах, що входять до складу ОЗС, з метою обґрунтування, в подальшому, можливих напрямків вдосконалення або створення нової системи технічного обслуговування та ремонту ТЗА, яка б відповідала стандартам, що прийняті в ОЗС НАТО.

Виклад основного матеріалу

Організація технічного та сервісного забезпечення ТЗА в Збройних силах України є важливим аспектом забезпечення обороноздатності країни та повинна бути відповідною до стандартів та принципів, прийнятих в ОЗС НАТО.

Достатньо великий об'єм та складність завдань, які повинні вирішуватися з використанням ТЗА, вимагають постійного підтримання справності наявного парку цього обладнання та підвищення ефективності його використання. Це досягається шляхом:

проведення своєчасного технічного обслуговування ТЗА згідно з регламентом;

проведення якісного ремонту та(або) модернізації наявної ТЗА, з використанням ремонтно-діагностичного обладнання та засобів вимірювання, що дозволяє при відносно невеликих фінансових витратах значно підвищити ефективність їх використання, продовжити їхній ресурс та терміни служби.

Так, наприклад, проведення модернізації комплексних апаратних зв'язку, радіорелейних станцій призводить до поліпшення їхніх технічних характеристик, зниження експлуатаційних витрат, підвищення бойової ефективності, бойових можливостей, безпеки використання тощо.

Зважаючи на сучасний фінансово-економічний стан нашої держави стає очевидним, що проведення своєчасного технічного обслуговування ТЗА згідно з регламентом та ремонту ТЗА за технічним станом агрегатним методом наразі є найбільш доцільним в Збройних силах України.

Проведений аналіз останніх досліджень та публікацій з цього напряму показав, що в ОЗС НАТО зараз приділяють надзвичайну увагу забезпеченню заданого рівня якості ТЗА, що у сучасних умовах можливе лише завдяки комплексному системному підходу до управління системою ТОР через впровадження систем управління якістю (далі – СУЯ) на всіх стадіях життєвого циклу ТЗА [16–18]. Саме на такому підході ґрунтується діяльність НАТО щодо створення та експлуатації систем озброєння, яка передбачає стандартизацію технологічних процесів і технічних рішень та розробку нормативних документів на відповідність вимогам, які перевіряють озброєння та військову техніку (далі – ОВТ) під час їх сертифікації.

Ефективність організації технічного та сервісного забезпечення ТЗА, а саме специфічний вміст їхньої елементної бази, визначають ряд особливостей у плануванні якості ТОР. Тому систему управління якістю ТОР можливо розглядати як замкнуту динамічну систему, в якій за допомогою контролю одержують інформацію про поточний стан ТЗА та здійснюють прогноз її стану. На основі цієї інформації приймають рішення про вид необхідних операцій (заходів), які можуть охоплювати дії як з попередження відмови (профілактиці), так і з відновлення властивостей після відмови.

Для отримання достовірної інформації щодо «вузьких місць» та реального стану справ у СУЯ будь-якого процесу будь-якої організації у світовій практиці менеджменту якості широко використовують статистичні методи управління якістю (так звані «інструменти якості»). Одним із найбільш ефективних з них є діаграма Ішикави («риб'яча кістка») [19], основною перевагою якої є її наочність та простота формування. Під час її побудови можливо використовувати показник пріоритетного числа ризиків (далі – ПЧР), що характеризує критичність невідповідності. ПЧР є узагальненою кількісною оцінкою комплексного ризику невідповідності та характеризується: значимістю (критичністю) наслідків невідповідності для споживачів – S [*significance* – значимість]; імовірністю виникнення причини невідповідності – O [*origination* – початок, походження; *originate* – виникати]; імовірністю виявлення причини – D [*detection* – виявлення]. Показники S, O, D визначаються експертами за спеціально розробленими 10-бальними шкалами, які складаються у формі таблиці або графіка. ПЧР причини розраховується як добуток цих трьох рангів і може приймати значення від 1 до 1000. Ті причини, у яких ПЧР більше ніж задане граничне значення, підлягають усуненню першочергово [19].

Авторами за участі експертів з використанням діаграми Ішикави було визначено основні фактори, які впливають на організацію технічного й сервісного забезпечення ТЗА та якості проведення ТОР (рис. 1) [15].

Як видно з отриманої діаграми, усю сукупність факторів, які впливають на організацію технічного та сервісного забезпечення ТЗА та якості проведення ТОР, можливо умовно об’єднати до таких груп, як: нормативно-правова база; людські фактори; технічні, технологічні та матеріально-технічні фактори; економічні та соціальні фактори; організаційні та структурні фактори; експлуатаційні фактори.

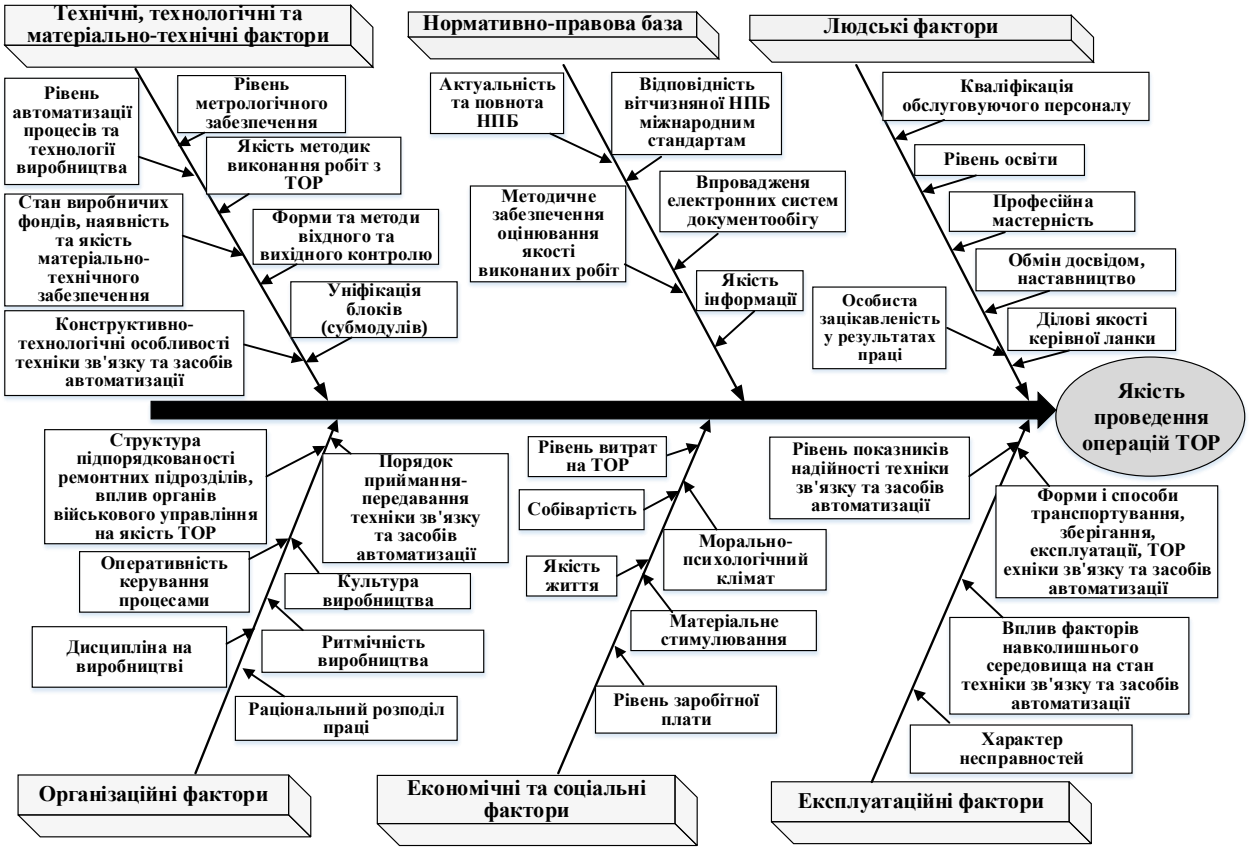

Рис. 1. Визначення основних факторів, які впливають на організацію технічного та сервісного забезпечення техніки зв’язку і засобів автоматизації та якості проведення ТОР

Проведений аналіз стану техніки зв’язку і засобів автоматизації, організації та проведення їхнього технічного обслуговування та ремонту з використанням методів діагностування та існуючого ремонтно-діагностичного обладнання у Збройних силах України [8] показав, що система ТОР не повною мірою задовольняє потреби військ навіть у мирний час через недостатнє фінансування, витрату та несвоєчасне поповнення ресурсу ТЗА, зменшення обсягу постачання ЗІП, військово-технічного майна, експлуатаційно-витратних матеріалів, недостатню професійну підготовку фахівців ремонтних підрозділів, використання застарілого ремонтно-діагностичного обладнання, скорочення термінів служби та ін.

Тому для розв’язання дійсних протиріч необхідний новий підхід до організації технічного та сервісного забезпечення ТЗА у напрямках: зменшення вартості проведення ТОР завдяки удосконаленню діагностичного забезпечення (далі – ДЗ), забезпечення необхідного рівня ремонтопридатності перспективних зразків ТЗА протягом всього їхнього життєвого циклу (далі – ЖЦ).

На сьогодні процеси ТОР відносять до основних об’єктів системи інтегрованої логістичної підтримки (далі – ІЛП), яка є складовою частиною PLM (Product Life-cycle Management) – «управління життєвим циклом виробу» або CALS-технологій *(Continuous Acquisition and Life-Cycle Support – інформаційної підтримки життєвого циклу продукції на всіх його стадіях)* (рис. 2).

ТЗА в загальному вигляді, враховуючи рівень науково-технічного прогресу та розвиток технологій, які були використані при їх розробці та виробництві, є складними технічними системами (далі – СТС). Ідея «управління життєвим циклом складних технічних систем» постійно розвивається і нині перетворилася на глобальну бізнес-стратегію підвищення ефективності бізнес-процесів завдяки інформаційній інтеграції і системному використанню інформації на всіх етапах життєвого циклу ТЗА.

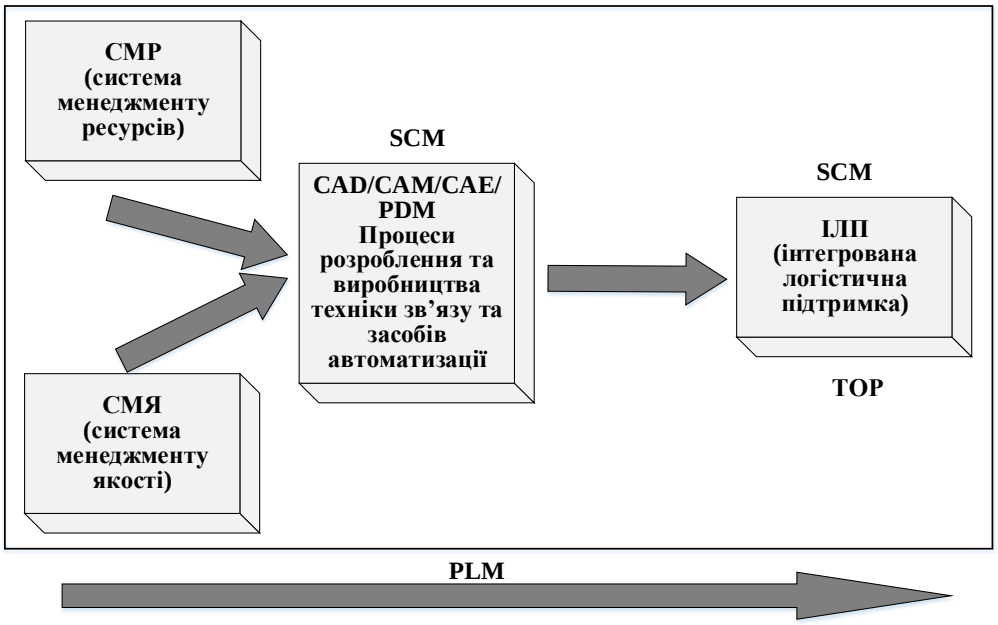

Рис. 2. Компоненти системи управління життєвим циклом ТЗА

Як показує вітчизняний та зарубіжний досвід, одним із найефективніших методів, що забезпечує високу якість функціонування СТС при одночасному зниженні вартості їх ЖЦ, є впровадження на всіх стадіях цього циклу засобів і методів автоматизованого контролю та визначення їхнього технічного стану.

Основною задачею, яка має вирішуватися використанням даного підходу, є збір, обробка та передача зацікавленим сторонам інформації, зокрема: результати діагностування, оцінки та прогнозування технічного стану СТС, пошуку та локалізації несправностей СТС тощо.

Відомо, що збір та обробка інформації про технічний стан СТС проводиться з метою:

розробки заходів, спрямованих на підвищення якості ремонту (відновлення) та зниження витрат на його проведення;

розробки заходів, спрямованих на дотримання правил технічної експлуатації ТЗА та підвищення ефективності функціонування системи ТОР.

Задачами, які мають вирішуватися під час збору та обробки інформації про технічний стан ТЗА як СТС, є:

визначення та оцінка показників якості ТЗА;

визначення конструкційних та технологічних недоліків, що знижують якість зразка ТЗА;

встановлення агрегатів та деталей, що обмежують надійність зразка ТЗА в цілому;

прогнозування виникнення відмов ТЗА залежно від умов та режимів їх експлуатації;

корегування показників надійності ТЗА;

оптимізація логістичного забезпечення та удосконалення системи ТОР в системі ІЛП;

визначення ефективних заходів, спрямованих на досягнення необхідних значень показників надійності.

Для досягнення зазначених цілей та реалізації завдань діагностування СТС необхідно розробити організаційно-технічні заходи та відповідний склад апаратних засобів для забезпечення отримання достовірної інформації зі зворотнім зв'язком щодо технічного стану ТЗА як СТС.

До відомостей, які підлягають збору, обробці та аналізу, відносяться дані:

про фактичні показники надійності ТЗА та їхніх складових частин, у тому числі дані про види, причини і наслідки відмов;

про фактичні показники ремонтопридатності ТЗА та їхніх компонентів, у тому числі дані про фактичні витрати часу на ремонт компонентів ТЗА та відновлення працездатності.

Як показує світова і вітчизняна практика розробки та виготовлення складних сучасних радіоелектронних засобів озброєнь, таких як апаратура та комплекси зв'язку, спецзв'язку, радіоелектронного управління, засоби автоматизації та ін., а також забезпечення високого рівня готовності та ефективності їх застосування вимагають не тільки великих людських та матеріальних витрат, а й вказують на:

наявність серйозних недоліків в їх експлуатації, організації технічного та сервісного забезпечення ТЗА, відновлення працездатності та постачання ЗІП (особливо у Збройних силах України та інших силових структурах);

збільшення термінів експлуатації існуючих зразків ТЗА, зниження якості експлуатації, а також значне зниження обсягів випуску нових зразків;

недосконаліть системи економіко-логістичних відносин із заводами-виробниками, що призводить до підвищення вартості експлуатації та відновлення працездатності ТЗА.

Завдання скорочення цих витрат при забезпеченні ефективності використання ТЗА є першочерговим для забезпечення безпеки країни.

Техніко-економічні, економічні та експлуатаційні характеристики наявної ТЗА можливо пов'язати інтегральним показником ефективності використання (E), який являє собою відношення ефективності використання засобів зв'язку (технічної ефективності) (E_T) до вартості життєвого циклу (далі – ВЖЦ).

Критерій «ефективність використання» характеризує міру доцільності застосування системи в складі ТЗА і в спрощеному вигляді може бути представлений добутком 3-х імовірнісних показників:

імовірності того, що працююча система буде безперервно функціонувати протягом строку служби – «надійність»;

імовірності того, що система готова до виконання завдання в довільний момент часу – «готовність до використання»;

імовірності того, що у процесі функціонування система успішно виконає своє завдання – «здатність до виконання завдань за призначенням».

Ефективність використання (E) визначається за формулою (1):

$$E = \frac{E_T}{ВЖЦ} = \frac{P_Г \cdot P_Н \cdot P_{ЗП}}{C_{ЗВ} + C_{КВДО} + C_{ЕВ}}, \quad (1)$$

де E_T – технічна ефективність;

$P_Г$ – ймовірність працездатності об'єкта в довільний момент часу – «коефіцієнт готовності»;

$P_Н$ – ймовірність безперервного функціонування об'єкта – «надійність»;

$P_{ЗП}$ – ймовірність правильного функціонування об'єкта – «здатність до виконання завдань за призначенням»;

$C_{ЗВ}$ – закупочна вартість;

$C_{КВДО}$ – капітальні витрати на контрольно-діагностичне обладнання;

$C_{ЕВ}$ – експлуатаційні витрати.

Необхідні значення показника *E* забезпечуються системою технічної експлуатації, що містить інформаційно-вимірювальні підсистеми (далі – ІВП), та реалізують функції визначення технічного стану при проведенні ТОР.

Прийнята система критеріїв дозволяє однозначно визначати загальну ефективність використання ТЗА та реалізувати їх порівняння за техніко-економічними показниками. Так, при однакових параметрах технічної ефективності, системи з вищими ВЖЦ мають нижчий показник загальної ефективності (*E*). Необхідність підвищення загальної ефективності використання ТЗА в умовах обмеження фінансових ресурсів вимагає, з одного боку, забезпечення високого рівня готовності до використання цих засобів за призначенням, надійності та ефективності їх застосування, а з іншого боку – досягнутих значних розмірів. Актуальність задачі полягає в тому, що зі зростанням складності ТЗА, а саме – застосовуванням при їх побудові нової елементної бази (НВІС, ПЛІС, елементи пам'яті, мікропроцесори), значно зростають часові і матеріальні витрати на проведення діагностувальних, регулювальних та ремонтно-відновлювальних робіт, приймально-здавальних випробувань при виробництві, використання ТЗА в різних умовах експлуатації.

Сучасний стан наявних засобів контролю, діагностування та іншого ремонтно-діагностичного обладнання, які використовуються при виробництві та забезпеченні подальшої експлуатації ТЗА, показує низький рівень автоматизації обладнання, яке використовується для цих цілей, є вузькоспеціалізованим, малопродуктивним і вимагає наявність підготовлених висококваліфікованих фахівців.

Аналіз джерел щодо експлуатації ТЗА як в Збройних силах України, так і в ОЗС НАТО, показує, що підвищення надійності та готовності до використання можна забезпечити відповідно до ***принципів системи менеджменту якості системи ТОР*** поліпшенням ремонтопридатності завдяки раціональному компонуванню об'єктів ТЗА та якісному ДЗ (рис. 3).

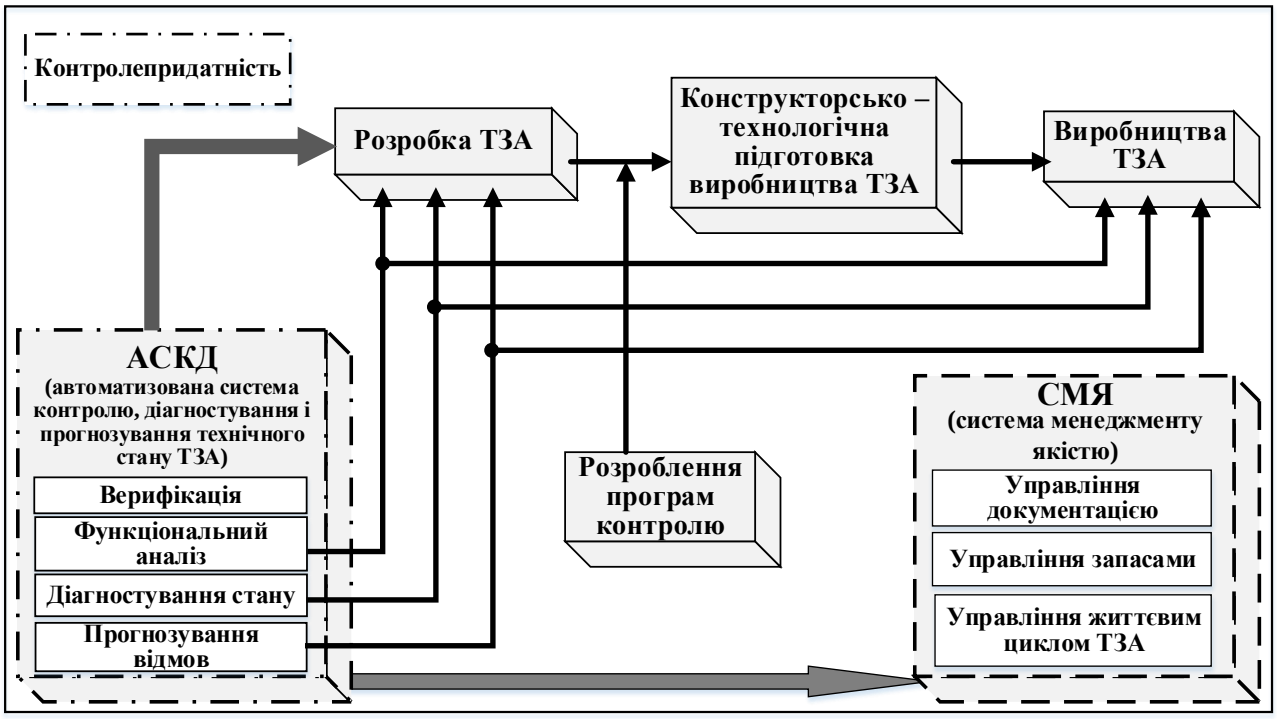

Рис. 3. Система менеджменту якості ТЗА з використанням автоматизованої системи контролю, діагностування і прогнозування технічного стану ТЗА на етапах ЖЦ

Вимоги, висунуті до сучасних систем діагностування та ремонту ТЗА та інших об'єктів комунікаційних систем, зокрема, передбачають мінімальну вартість відновлення об'єктів за час, який не перевищує заданого експлуатаційно- технічними характеристиками.

Існуюча система технічного діагностування лише частково задовольняє необхідним вимогам на всіх етапах ЖЦ.

Є два напрямки зменшення часу відновлення. Перший передбачає удосконалення структурних зв'язків системи. Другий напрямок передбачає збільшення продуктивності ІЛП, а також зниження вартості і скорочення часу діагностування як найбільш вагомої складової часу відновлення.

Отже, для «управління життєвим циклом складних технічних систем» необхідне комплексне застосування автоматизованої системи контролю, діагностування і прогнозування (далі – АСКДП) технічного стану комплексу новітньої ТЗА.

Основою системи менеджменту якості системи ТОР є система розроблення та постановка на виробництво (далі – СРПВ) ОВТ, у даному випадку слід розглядати систему розроблення та постановку на виробництво ТЗА як і систему управління ЖЦ ТЗА, прийнятої в ОЗС НАТО [20; 21], ґрунтовано на принципах: пріоритетності використання системи управління ЖЦ ОВТ (commitment to systems life cycle management). Цей принцип вимагає від замовника, виконавців та співвиконавців замовлення при виробництві ТЗА дотримання всіх правил і процесів, потрібних для досягнення визначених цілей, – співпраці та взаємодії (cooperation and interoperability). Замовник, виконавці та співвиконавці замовлення розробляють ТЗА, які своїми тактико-технічних характеристиками відповідають потребам оборони держави та взаємосумісні з засобами зв'язку, які використовуються в ОЗС НАТО.

Упровадження системи управління життєвим циклом ТЗА дає змогу задовольнити ці потреби через взаємодію та виконання вимог щодо їхньої стандартизації; ефективності (efficiency) використання ТЗА. Під ефективністю потрібно розуміти ефективне й економічне використання національних ресурсів та ресурсів держав-партнерів для створення ТЗА. Упровадження системи управління ЖЦ ТЗА дає змогу у найкращий спосіб здійснювати їх розроблення, виробництво, закупівлю, використання, підтримку та вилучення, – співпраці з промисловістю (collaboration with industry). Упровадження системи управління ЖЦ ТЗА потребує тісних робочих відносин з промисловістю, максимального використання цивільних стандартів (де це можливо), усебічного застосування сучасних інформаційних технологій та знань у різних сферах, співпраці замовника, виконавців та співвиконавців замовлення для оптимізації спільних витрат; — якості (quality) ТЗА. Оборонні спроможності держави значною мірою залежать від якості ТЗА. Якості ТЗА у найкращий спосіб можливо досягти за допомогою інтегрованого системного підходу впродовж усього ЖЦ ТЗА [22].

Для проведення в польових умовах операцій з технічного обслуговування та ремонту ТЗА пропонується використовувати універсальні апаратні технічного забезпечення (далі – АТЗ) модульного типу з елементами АСКД, які нині реально розробляються.

Під час проведення аналізу організації технічного та сервісного забезпечення ТЗА в країнах-членах НАТО виявлено, що планові види ремонту військових засобів зв'язку і автоматизації не проводяться. Це пов'язано, з одного боку, з тим, що засоби зв'язку і автоматизації будуються на сучасній елементній базі, яка дозволяє експлуатувати техніку без планових ремонтів до 5–10 років. З іншого боку, у зв'язку з інтенсивним розвитком інформаційно-телекомунікаційних технологій, за 5–10 років засоби зв'язку і автоматизації морально застарівають, тактико-технічні вимоги не відповідають сучасним вимогам і їх подальша експлуатація недоцільна. Тому планові види ремонту не проводяться, застарілі засоби зв'язку і автоматизації списуються й на озброєння приймаються нові, перспективні зразки.

Фінансування збройних сил країн-членів НАТО дозволяє здійснювати таку політику переозброєння.

У країнах-членах НАТО реалізація поточного (відновлювального) ремонту третього ступеню складності здійснюється завдяки впровадженню знеособленого трирівневого агрегатного методу ремонту із залученням цивільних підприємств та організацій.

У сухопутних військах країн НАТО проводяться три види ремонту: 1-й рівень – військовий; 2-й рівень – польовий; 3-й рівень – базовий (капітальний).

На **першому рівні** ремонт виконується штатним екіпажем на місці експлуатації техніки з глибиною пошуку дефекту до блоку.

Тобто завдання екіпажу, який експлуатує даний засіб зв'язку і автоматизації, – виявити за допомогою вбудованих засобів діагностування несправний блок (у випадку моноблоку – виявити факт його несправності), вилучити його, обміняти встановленим порядком на справний блок (моноблок) у військовому ремонтному органі, встановити на штатне місце та, за потреби, здійснити штатні регулювання.

Подальший ремонт блоків не впливає на боєготовність засобів зв'язку і автоматизації, які за час ремонту вже експлуатуються в штатному режимі.

На **другому рівні** несправний блок ремонтується у військових ремонтних органах на пунктах технічного обслуговування і ремонту (далі – ПТОР) – у стаціонарних умовах, та у польових умовах з використанням апаратних технічного забезпечення шляхом виявлення і заміни несправного модулю – з використанням типового елементу заміни (далі – ТЕЗ) агрегатним методом. Для організації ремонту ТЗА на цьому рівні необхідно створення підмінного фонду блоків та ТЕЗ. Відремонтований блок, шляхом виявлення і заміни несправного ТЕЗ, поповнює підмінний фонд блоків, який створено у військовому ремонтному органі. Виявлений несправний ТЕЗ встановленим порядком направляється на третій рівень ремонту.

Третій рівень базовий (капітальний) ремонту здійснюється шляхом пошуку та заміни несправного невідновлювального елемента (електрорадіоелемента) в несправних ТЕЗ в умовах регіонального сервісного центру чи в польових умовах при проведенні ремонту агрегатним методом.

Третій рівень ремонту здійснюється в регіональних сертифікованих сервісних центрах, які укомплектовані висококласним ремонтним персоналом, спеціальними засобами вимірювальної техніки і обладнанням та технологічними ремонтними лініями.

Відремонтовані ТЕЗ направляються назад до військового ремонтного органу для відновлення підмінного фонду ТЕЗ. Доставка несправних ТЕЗ до регіональних сервісних центрів та повернення відремонтованих у військовий ремонтний орган може здійснюватися за домовленістю силами і засобами як сервісних центрів, так і військових ремонтних органів.

Регіональні сервісні центри в країнах НАТО створені на базі цивільних підприємств та організацій різних форм власності на договірних засадах з пріоритетним наданням цього права організаціям-розробникам та виробникам цих засобів.

Схема організації технічного та сервісного забезпечення ТЗА в країнах НАТО показана на рисунку 4.

В деяких країнах НАТО **другий рівень розділяється на два рівні: другий та третій.** При цьому **на третьому рівні** проводиться діагностування пристрою за допомогою спеціальних вимірювально-діагностичних засобів, заміна несправних модулів здійснюється особовим складом військового ремонтного органу (екіпажу АТОР) з використанням агрегатного методу.

Операції, визначені на **третьому рівні базовому (капітальному),** проводяться відповідно на **четвертому рівні** в повному обсязі [23].

Особлива увага в ОЗС НАТО приділяється підготовці кваліфікованих кадрів. Завдяки вдосконаленню організаційно-штатної структури ремонтних органів, оснащення їх новітніми ремонтно-діагностичними засобами, а також збільшення кількості підготовки фахівців-ремонтників надало можливість збільшити кількість відремонтованої ОВТ на 10–15 %.

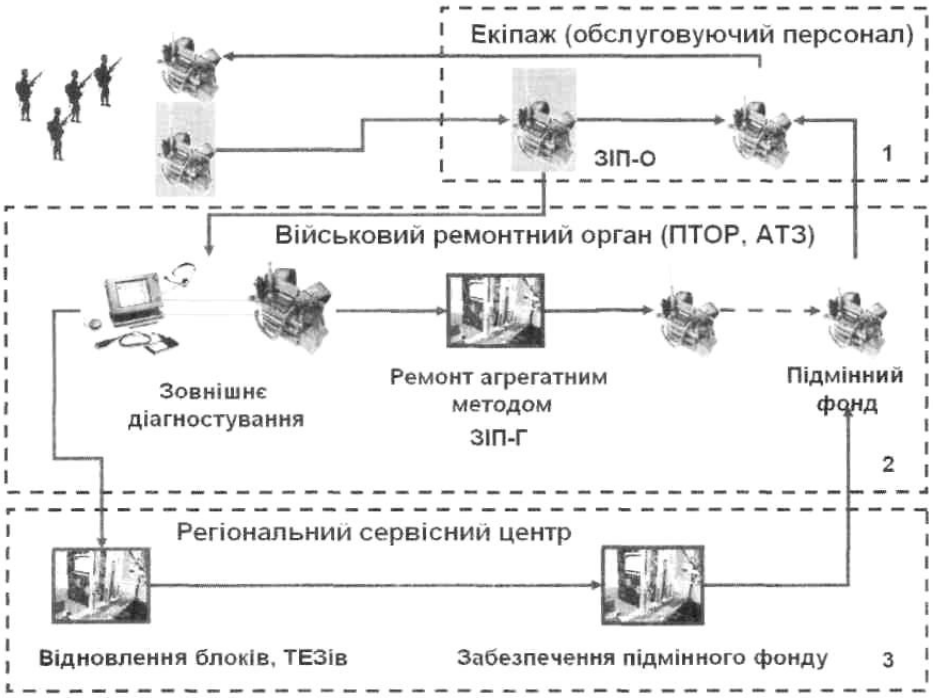

Рис. 4. Схема організації технічного та сервісного забезпечення ТЗА в країнах НАТО

Наприклад, у Великій Британії вузи та училища щорічно випускають до 1200 фахівців інженерно-технічних посад для ремонтно-відновлювальної служби. У Німеччині є три такі школи, в одній з яких здійснюється перепідготовка фахівців всіх видів військових сил з технічного обслуговування ОВТ. Навчання ведеться за 114 програмами. Удосконалення процесу підготовки фахівців ведеться, насамперед, у напрямку інтенсифікації навчання. Технічні засоби навчання, що використовуються в ОВС НАТО для підготовки кваліфікованих кадрів, залежно від призначення розділяють на інформатори, репетитори, контролери та тренажери. Тренажери, на думку фахівців, призначені для прищеплення практичних навичок роботи з ОВТ, закріплення знань і підтримки професійних навичок шляхом періодичних тренувань. В ОЗС НАТО розробляються тренажери різних видів: одні призначені для навчання окремих фахівців (ремонтників зв'язку і АСУ та інших), а інші – екіпажів в цілому.

Так, прийнята в арміях держав НАТО система технічного забезпечення ТЗА дозволяє успішно вирішувати наступні завдання: проводити агрегатним способом ремонт техніки зв'язку при виході її з ладу на місцях або на збірних пунктах, що дозволяє скоротити час її відновлення; рівномірно розподіляти обсяг робіт між ланками системи ремонту та сервісу.

Загалом, відповідно до оцінки закордонних експертів, діюча нині в арміях держав НАТО система технічного забезпечення засобів зв'язку та якість підготовки фахівців ремонтників спроможні забезпечити своєчасне і повне управління з'єднаннями і частинами в умовах сучасної війни.

Провівши аналіз керівних документів, слід зазначити, що нормативно-правова база, сформована на основі системи стандартів, узгоджується з актами національного законодавства України в цілому, враховуючи перетворення, які сталися в економці, тенденції та шляхи розвитку, прийняті в ОЗС НАТО.

Досвід бойових дій показав, що всі польові вузли зв'язку тактичної ланки управління підрозділів сил оборони держави розгорнуті на базі комплексних апаратних зв'язку, переобладнаних сучасними засобами електронних комунікацій, які забезпечують відкритий та засекречений автоматичний телефонний зв'язок, відкриту та захищену передачу даних, захищений відеоконференційний зв'язок, доступ до мережі ІСД Інтернет відповідним

посадовим особам пунктів управління підрозділів Збройних сил України обсягом, достатнім для виконання завдань за призначенням.

Так, наприклад, матеріально-технічна допомога від уряду США шляхом постачання радіозасобами виробництва компанії Harris різних типів дала змогу наростити існуючу систему зв'язку Збройних сил України та забезпечити захищеним цифровим короткохвильовим та ультракороткохвильовим радіозв'язком підрозділи Збройних сил України.

Провівши аналогію щодо етапів створення системи технічного забезпечення засобів зв'язку в ОЗС НАТО, можемо визначити такі головні критерії:

стандартизація техніки зв'язку і автоматизації;

повнота і своєчасність забезпечення частин сучасною технікою;

якісна підготовка фахівців;

мінімальний час для відновлення пошкоджених ТЗА.

Досвід проведення бойових дій підтверджує необхідність проведення ремонту ТЗА під час виконання завдань тільки за умови відповідності системи ТОР Збройних сил України, прийнятій в ОЗС НАТО, коли:

військовий ремонт (рівень екіпажу) проводиться шляхом легкого поточного ремонту матеріальної частини з використанням ЗІП;

польовий ремонт (рівень майстерні) передбачає тільки заміну або ремонт агрегатним методом виробів, що вийшли з ладу зі складу апаратних;

базовий ремонт (рівень підприємства) виконується на підприємствах, що виготовляють техніку зв'язку з метою відновлення або заміни основних вузлів і агрегатів.

У процесі виконання державних програм розвитку технічного та сервісного забезпечення ТЗА, після уточнення їхніх показників відповідно до положень «Концепції Державної цільової програми реформування та розвитку оборонно-промислового комплексу», стає очевидним і створення нової системи ТОР у Збройних силах України та інших складових сил оборони держави, відповідно до якої середній та капітальний ремонт ТЗА необхідно проводити на ремонтних підприємствах Збройних сил України, в першу чергу – на державних підприємствах, а поточний – у військових частинах.

Під час проведення аналізу діючої системи ТОР в Збройних силах України реалізації основних принципів щодо технічного обслуговування та ремонту в ОЗС НАТО та шляхів їх імплементації в нормативно-правову базу держави можемо виділити основні пріоритетні напрямки організації технічного та сервісного забезпечення ТЗА в Збройних силах України, які повинні містити:

1. Модернізацію та удосконалення існуючої інфраструктури зв'язку для забезпечення стійкості та надійності зв'язку в умовах бойових дій з використанням новітньої техніки зв'язку і засобів автоматизації.

2. Розвиток та впровадження сучасних технологій зв'язку, зокрема систем широкосмугового доступу, супутникових систем, мережі 5G, інтернету бойових речей та інших інноваційних рішень.

3. Забезпечення кібербезпеки та захисту інформаційних ресурсів від хакерських атак та кіберзагроз у техніці зв'язку і засобах автоматизації, що використовуються.

4. Розвиток та вдосконалення систем автоматизації управління, що дозволить ефективніше координувати дії військових ремонтних підрозділів та забезпечувати оперативність прийняття рішень.

5. Впровадження сучасних засобів телекомунікаційного забезпечення для покращення обміну інформацією між військовими ремонтними підрозділами та командуванням.

6. Створення та забезпечення функціонування автоматизованої системи контролю, діагностування і прогнозування (далі – АСКД) технічного стану ТЗА в складі новостворюваної системи технічного обслуговування та ремонту ТЗА.

7. Упровадження системи управління ЖЦ ТЗА на кшталт використання таких систем у ОЗС НАТО.

8. Розробку, впровадження автоматизованої системи моніторингу та обліку ТЗА з подальшою інтеграцію її в систему ТОР, що дозволить вести ефективний контроль за станом ТЗА та проведенням їх відновлення (ремонту).

9. Розробка сучасних (модернізації існуючих) апаратних технічного обслуговування та ремонту ТЗА модульного типу.

10. Підготовка та підвищення кваліфікації персоналу військових ремонтних підрозділів з питань організації технічного та сервісного забезпечення ТЗА.

11. Розвиток та вдосконалення системи постачання запасних частин та матеріалів для ТЗА.

12. Забезпечення створення та підтримання резерву ТЗА, формування ЗІП для вирішення невідкладних завдань та мінімізації часу на відновлення техніки.

13. Впровадження (імплементація) стандартів та нормативних документів НАТО щодо технічного та сервісного забезпечення ТЗА.

Це лише деякі можливі напрямки організації технічного та сервісного забезпечення ТЗА в Збройних силах України. Конкретний їх перелік та пріоритетність можуть визначатися відповідно до потреб та набуття спроможностей Збройними силами України.

Разом з переозброєнням підрозділів сил оборони держави новітньою ТЗА має бути забезпечена модернізація існуючих і розробка та налагодження виробництва вітчизняних засобів, тактико-технічні характеристики яких будуть відповідати сучасним вимогам.

В умовах реформування Збройних сил України, одночасно зі зміною підходів щодо ремонту техніки зв’язку, в тому числі і новітньої, наприклад, агрегатним способом, та з переходом на сервісне обслуговування необхідно врахувати і наявний досвід провідних держав світу щодо навчання фахівців зв’язку (під час отримання ними на озброєння нової техніки), та враховуючи проведений аналіз стану організації технічного та сервісного забезпечення ТЗА під час проведення бойових дій по відсічі широкомасштабної збройної агресії рф, пропонується:

Збройним силам України та іншим складовим сил оборони держави перейти до системи ремонту та сервісного обслуговування за технічним станом.

Система технічного забезпечення щодо ТОР ЗЗА повинна мати основні пріоритетні напрямки розвитку та вирішувати наступні **завдання:**

розроблення нових нормативних і керівних документів, а саме: впровадження змін шляхом послідовного опрацювання і прийняття відповідних взаємоузгоджених актів законодавства, державних стандартів, технічних регламентів, актів центральних органів виконавчої влади для організації системи розроблення, поставлення на виробництво та організації ремонту військової техніки у відповідних підрозділах сил оборони держави;

впровадження на інформаційно-телекомунікаційних вузлах Збройних сил України та інших складових сил оборони держави автоматизованих систем технічної підтримки [14];

розроблення і запровадження перспективних діагностичних систем;

поступовий перехід від планового ремонту засобів зв’язку на ремонт за технічним станом, застосування агрегатного методу поточного та відновлюваного ремонту;

забезпечення повнофункціональної роботи сервісних центрів (підрозділів) технічного обслуговування і ремонту на базі ремонтних установ, військових частин із залученням представників виробників сучасних та перспективних засобів зв’язку;

перехід від широкої номенклатури спеціалізованих апаратних технічного обслуговування та ремонту старого парку до розробки комплексної апаратної технічного обслуговування та ремонту модульного типу, яка буде використовуватися для проведення обслуговування та ремонту усього парку існуючих та перспективних засобів ТЗА в польових умовах;

забезпечення всіх військових ремонтних органів зв'язку ремонтною та експлуатаційною документацією на новітні засоби зв'язку, спеціальними сучасними засобами вимірювально-діагностичного обладнання, ремонтними комплектами до сучасних засобів та проведення навчання особового складу щодо набуття навичок та освоєння нових методів ремонту відповідної ТЗА;

стандартизація процесів розробки, виробництва, постачання та експлуатації цифрових комплексів та засобів зв'язку;

уніфікація та стандартизація цифрових комплексів та засобів зв'язку, елементної бази, операційних систем і програмних модулів.

Висновки. Отже, у цій статті проведено аналіз ефективності організації технічного та сервісного забезпечення ТЗА в Збройних силах України.

Розглянуто можливість впровадження системи менеджменту якості з використанням автоматизованої системи контролю, діагностування і прогнозування технічного стану ТЗА на етапах ЖЦ.

У процесі проведення аналізу діючої системи ТОР в Збройних силах України та аналізу реалізації основних принципів щодо технічного обслуговування та ремонту в ОЗС НАТО визначено основні шляхи їх імплементації в нормативно-правову базу держави, розглянуто основні пріоритетні напрямки організації технічного та сервісного забезпечення ТЗА в Збройних силах України.

У статті зроблено акцент на можливості упровадження системи управління ЖЦ ТЗА задля забезпечення більш ефективного використання ТЗА.

Зроблено загальний висновок про те, що Збройним силам України та іншим складовим силам оборони держави необхідно перейти до системи ремонту та сервісного обслуговування за технічним станом.

Визначено пріоритетні напрямки та завдання перспективної системи ТОР ТЗА.

Перспективи подальших досліджень. Перспективи подальших досліджень вбачають у проведенні дослідження можливості застосування автоматизованої системи контролю, діагностування і прогнозування технічного стану ТЗА, аналізу підходів до оцінки ефективності використання ремонтно-відновлювальних засобів в польових умовах та імплементації нормативно-правової бази, прийнятої в ОЗС НАТО в новітню систему ТОР ТЗА Збройних сил України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про рішення Ради національної безпеки і оборони України від 20.08.2021 «Про Стратегічний оборонний бюлетень України»: Указ Президента України від 17.06.2021 № 473/2021.

2. Концепція Державної цільової програми реформування та розвитку оборонно-промислового комплексу України на період до 2020 року: розпорядження Кабінету Міністрів України від 20.01.2016 № 19–р.

3. Про затвердження Порядку відновлення, ремонту, модернізації, збільшення установленого ресурсу та продовження строку служби (зберігання) озброєння, військової і спеціальної техніки, за якими не здійснюється авторський нагляд: Постанова Кабінету Міністрів України від 20.03.2015 № 135 (зі змінами).

4. Про схвалення Основних напрямів розвитку озброєння та військової техніки на довгостроковий період: розпорядження Кабінету Міністрів України від 14.06.2017 № 398-р (зі змінами).

5. Про затвердження Порядку логістичного забезпечення сил оборони під час виконання завдань з оборони держави, захисту її суверенітету, територіальної цілісності та недоторканості: Постанова Кабінету Міністрів України від 27.12.2018 № 1208.

6. Про рішення Ради національної безпеки і оборони України від 25.03.2021 «Про Стратегію воєнної безпеки України»: Указ Президента України від 25.03.2021 № 121/2021.

7. Опенько П. В., Поліщук В. В., Миронюк М. Ю. Досвід застосування адаптивних стратегій технічного обслуговування і ремонту озброєння та військової техніки в державах-членах НАТО // Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки. 2021. № 2 (8) С. 101–111.

8. Івченко М. М., Яровий В. С., Гришина Н. С., Ткач В. О., Побережець Т. В. Напрями вдосконалення системи технічного обслуговування засобів зв'язку та АСУ ЗС України // Збірник наукових праць ВІТІ. 2019. № 1. С. 18–22.

9. Морозов О. О. Наукові засади розвитку технічного забезпечення у Національній гвардії України // Науковий вісник Київського інституту Національної гвардії України.

10. Власов І. О., Воробйов О. М., Наконечний О. В., Середа Ю. С. Обґрунтування концептуальних та наукових підходів щодо розвитку єдиної системи логістики в Збройних Силах України // Збірник наукових праць Харківського національного університету Повітряних Сил ім. Івана Кожедуба. 2020. № 2 (64). С.12–18.

11. Закалад М. А., Педан Ф. П., Романченко О. А. Підходи до формування основних характеристик АСУ логістичного забезпечення ЗС України // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України ім. Івана Черняховського. 2018. № 1 (62). С. 97–101.

12. Гриб Д. А., Ланецький Б. М., Лук'янчук В. В. Удосконалення методів технічної експлуатації і ремонту як основа підтримання боєготового стану озброєння в сучасних умовах // Наука і оборона. 2012. № 3. С. 55–63.

13. Smith A. M. RCM: gateway to world class maintenance / Anthony M. Smith., Glenn R. Hincheliffe. Elsevier Inc., Burlington, USA, 2004. 340 p.

14. Клімушин П. С., Кротов В. Д. Автоматизована система управління Збройних сил України як сучасний різновид стратегічного озброєння // Теорія та практика державного управління. 2014. Вип. 1 (44). С. 16–23.

15. Ткаченко Л. А. Системи управління якістю підприємств сфери інжинірингу: монографія. Одеса: ОНЕУ, 2019. 378 с.

16. Капінос Г. І., Грабовська І. В. Управління якістю: навч. посіб. Київ: Кондор-Вид., 2016. 278 с.

17. Управління якістю: підр. / за ред. П. П. Вороб'єнко, І. В. Станкевич, Є. М. Стрельчук, О. І. Глухова. Одеса: ОНАЗ, 2014. 376 с.

18. Ліфіц І. М. Стандартизація, метрологія та підтвердження відповідності: підручник та практикум. 13-те вид. Вид-во «Юрайт», 2019. 363 с.

19. Кане М. М. Системи, методи та інструменти менеджменту якості: навч. посіб. / за ред. М. М. Кане., Б. В. Іванов, В. М. Корешков, А. Г. Схиртладзе. П., 2008. 560 с.

20. C-M(2005)0108-AS1 NATO policy for systems life cycle management.

21. AAP-03:2015 Production, maintenance and management of NATO standardization documents.

22. ДСТУ В-П 15.001:2018. Система розроблення і поставлення на виробництво озброєння та військової техніки.

23. Розширений каталог служби технічної підтримки корпорації Harris // Технічні комунікації та каталог продукції Harris в світі – 2020 / США. 2019.

УДК 004.054

Карпенко А. О. (ВІТІ ім. Героїв Крут)
Мусієнко В. А. (ВІТІ ім. Героїв Крут)
Краснобокий А. В. (ВІТІ ім. Героїв Крут)
Тітаренко А. В. (ВІТІ ім. Героїв Крут)

АНАЛІЗ МЕТОДІВ ОЦІНКИ ВИТРАТ ПІД ЧАС РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА РАННІХ ЕТАПАХ ПРОЄКТУВАННЯ

Сучасний світ неможливо уявити без програмного забезпечення. Від мобільних додатків до складних корпоративних систем, програмне забезпечення відіграє критичну роль у всіх сферах життя і бізнесу. З кожним роком збільшується розмір та складність інформаційних проєктів, що ставить перед індустрією розробки низку складних завдань.

Один із головних викликів, які постають перед командами розробників, це вірна оцінка витрат на ранніх етапах проєктування. Недооцінка або переоцінка витрат можуть призвести до перевищення бюджету, затримок у виконанні та загрожувати успішності всього проєкту. Точна оцінка є необхідною для забезпечення чіткого планування та ефективного управління розробкою програмного забезпечення.

Ця стаття присвячена аналізу методів оцінки витрат при розробці програмного забезпечення на ранніх етапах проєктування. У цій роботі розглядаються такі методи оцінки, як метод експертної оцінки, референтних проєктів, функціональних точок «знизу-вгору» та параметрична оцінка. Було проведено порівняльний аналіз розглянутих методів, виявлено їхні переваги та недоліки. Якщо опустити дані про специфіку проєкту на ранніх етапах розробки, то оптимальним рішенням для оцінки вартості є метод функціональних точок. Він має високу точність оцінки, масштабованість, простоту у використанні та сумісність із проєктами різної ступені складності.

Результати дослідження можуть бути корисними для фахівців у сфері розробки програмного забезпечення та управління проєктами, допомагаючи їм вибрати необхідний метод оцінки програмних проєктів на ранніх стадіях. Визначені перспективні напрямки подальших досліджень.

Ключові слова: *програмне забезпечення, оцінка, метод, проєкт.*

A. Karpenko, V. Musiienko, A. Krasnobokyi, A. Titarenko Analysis of Cost Estimation Methods in Early Software Development Stages.

The modern world heavily relies on software, from mobile applications to complex corporate systems. Software plays a critical role in all aspects of life and business. With each passing year, the size and complexity of information technology projects continue to grow, posing a series of challenges to the development industry.

One of the main challenges faced by development teams is accurately estimating costs at the early stages of project planning. Underestimating or overestimating costs can lead to budget overruns, project delays, and jeopardize the overall success of the project. Accurate estimation is essential to ensure clear planning and effective management of software development.

This article is dedicated to the analysis of cost estimation methods in early stages of software development projects. In this work, we explore various estimation methods, including expert judgment, analogous estimation, function points, bottom-up estimation, and parametric estimation. We conducted a comparative analysis of these methods, identifying their advantages and disadvantages. When considering the specific project context at the early stages of development, the Function Points method emerges as the optimal choice for cost estimation. It offers high estimation accuracy, scalability, ease of use, and compatibility with projects of varying complexity.

The research findings can be valuable for professionals in the software development and project management fields, aiding them in selecting the appropriate estimation method for software projects in their early stages. The study also identifies promising directions for further research.

Keywords*: software, estimation, method, project.*

Постановка проблеми

Стрімкий розвиток інформаційних технологій призвів до збільшення кількості великих проєктів у сфері розробки програмного забезпечення (далі – ПЗ). Практика показує, що більшість проєктів закінчуються з порушенням графіку виконання або перевищенням бюджету. Тому дуже важливо на початкових етапах розробки оцінити потенційну вигоду та ризики, які пов’язані з проєктом, і провести аналіз можливих сценаріїв подій.

Однією з причин неправильної оцінки є відсутність необхідних знань у даній галузі. Невідповідний вибір методів та інструментів оцінки може призвести до неточних результатів, при цьому основні фактори та чинники можуть залишитися нерозглянутими. Без правильної оцінки стає неможливим забезпечення чіткого планування та ефективного управління проєктом. Важливо скласти точний прогноз тривалості проєкту, витрат та інших аспектів ще на стадії планування. Дуже часто оцінка розробки ПЗ ігнорується, що може спричинити серйозні проблеми та невдале завершення проєкту.

Невірна оцінка вартості, часу і ресурсів для створення ПЗ може призвести до недостатньої кількості учасників у проєктній команді, занадто стиснутих термінів розробки, і в кінцевому результаті, втрати довіри до розробників, особливо у випадку порушень графіка виконання. З іншого боку, якщо проєкту виділено більше ресурсів, ніж він фактично потребує, і це не супроводжується належним контролем щодо їхнього використання, то це може призвести до зростання вартості проєкту, що, в свою чергу, може спричинити затримки у завершенні проєкту. Тому потрібно правильно визначити обсяг зусиль, потрібних для успішної реалізації або підтримки програмного проєкту. Важливо пам’ятати, що початкова оцінка проєкту та узгоджений бюджет не є постійними і протягом всього життєвого циклу розробки вони будуть піддаватися змінам.

Підсумовуючи вищесказане, можна зробити висновок, що проблема полягає у правильному виборі методів та інструментів оцінки вартості ПЗ при проєктуванні.

Аналіз останніх досліджень і публікацій

Питання оцінки вартості програмного забезпечення набуло великого значення в наш час через різноманітність факторів, що впливають на процес розробки та експлуатації програмних продуктів. Так, згідно зі звітом [1] із статистичними даними щодо численних аспектів проєктів у сфері розробки ПЗ, 31 % проєктів завершились успішно, 50 % виявилися проблемними, 19 % не вдалося успішно реалізувати. Тому дуже важливо проводити правильну оцінку на початкових етапах.

У науковій статті [2] авторами розглянуто моделі, методи та засоби оцінки вартості ПЗ. В роботі [3] проаналізовано підходи оцінювання вартості програм для визначення їхньої ринкової вартості, використовуючи ПЗ на основі моделі COCOMO. У статті [4] розглянуто методи системного аналізу процесів створення ПЗ, методів і моделей визначення вартості ПЗ; проведено порівняння програмних засобів оцінки, що базуються на моделях SLIM та COCOMO.

Однак на сьогодні не проведено порівняльний аналіз методів оцінки вартості ПЗ на початкових етапах проєктування.

Метою статті є аналіз можливостей використання методів оцінки вартості розробки ПЗ та проведення їх порівняння для вибору оптимального.

Основна частина

Оцінка вартості розробки ПЗ на ранніх етапах проєктування є складним завданням, що полягає в передбаченні оптимальних зусиль, часових рамок і фінансових витрат, необхідних для успішної реалізації програмного продукту, а також його подальшого впровадження та підтримки. Цей процес вимагає уважного аналізу і врахування всіх важливих факторів, що впливають на проєкт, і гарантує, що ресурси виділяються раціонально і з урахуванням можливих ризиків.

Процес оцінки вартості є важливим початковим етапом у відносинах з підрядниками, які розробляють ПЗ. Правильно проведена оцінка встановлює надійну основу для всіх подальших рішень і кроків у процесі управління проєктом. Вона дозволяє уникнути непередбачених проблем та сприяє ефективному веденню проєкту.

Вартість проєкту містить такі складові:

вартість робочого часу – витрати на заробітну плату розробників, тестувальників, інженерів та іншого персоналу, який працює над проєктом;

тривалість проєкту – це час, необхідний для завершення всіх робіт над ПЗ;

витрати на інфраструктуру – охоплює витрати на обладнання, ПЗ, сервери, бази даних та інші технічні ресурси, необхідні для розробки, тестування та впровадження програми;

вартість матеріалів – витрати на ліцензії для сторонніх компонентів або бібліотек, які використовуються у програмному продукті;

підтримка і обслуговування – витрати на підтримку програмного продукту після впровадження, включаючи витрати на виправлення помилок, оновлення, технічну підтримку та обслуговування.

Якщо інвестор чи розробник ПЗ немає достатньо коштів, щоб фінансувати весь проєкт, це може призвести до невдачі або неповного завершення завдань. Важливо планувати і керувати фінансами уважно, щоб забезпечити успішну реалізацію програми.

Існує велика кількість проєктів у галузі розробки ПЗ, і кожен з них має унікальні вимоги, цілі та умови, тому не існує жодного універсального методу для точної оцінки витрат. Оцінювач повинен проаналізувати проєктну документацію та визначити, які підходи та технології розробки найкраще відповідають конкретним цілям проєкту. При оцінці витрат на розробку можуть використовуватися різноманітні методи для забезпечення точності оцінки проєкту і врахування всіх можливих факторів.

Методи оцінки вартості – це інструменти, які використовуються керівниками проєктів для проведення розрахунків загальних витрат проєкту на ранніх стадіях його створення або навіть до початку проєктування. Ці методи допомагають приймати обґрунтовані рішення щодо фінансових аспектів проєкту та планування ресурсів.

У цій роботі будуть розглянуті найпоширеніші методи, які використовують менеджери проєктів для оцінки їхньої вартості, а саме: експертна оцінка (Expert Judgment), метод референтних проєктів (Analogous Estimation), метод функціональних точок (Function Point Analysis), метод «знизу-вгору» (Bottom-Up Estimation) та параметрична оцінка (Parametric Estimation).

Метод експертної оцінки (Expert Judgment)

Експертна оцінка – це метод оцінки вартості ПЗ, при якому спеціалісти з великим досвідом та знаннями в галузі використовують свій експертний погляд для приблизного визначення витрат та обсягу робіт. Точність значною мірою залежить від досвіду та кількості задіяних в процесі експертів, чіткості планування робіт і кроків, а також від типу самого проєкту.

Розглянемо основні етапи даного методу:

вибір експертів – оцінка виконується експертами, які мають досвід і знання в області ПЗ. Важливо вибрати кваліфікованих і компетентних експертів, які можуть надати обґрунтовані оцінки;

збір і аналіз даних – експерти збирають необхідні дані про проєкт, які можуть містити обсяг робіт, тривалість проєкту, ресурси, технічні вимоги та інші фактори, що впливають на вартість;

формування оцінки – на основі зібраних даних і аналізу експерти формують оцінку вартості ПЗ;

подання результатів – оцінка вартості ПЗ та відповідні висновки надаються клієнту для прийняття рішення;

перевірка та коригування – у деяких випадках може знадобитися перевірка та коригування оцінки на основі додаткової інформації або змін у проєкті.

Основні ситуації, коли може бути корисно використовувати даний метод:

на початкових стадіях проєкту – коли деталізована інформація про проєкт ще не повністю визначена і відсутні необхідні дані для застосування більш точних методів оцінки. Експерти можуть дати приблизну оцінку вартості та обсягу робіт на цій стадії;

у випадку невеликих проєктів – для невеликих або короткострокових проєктів може бути недоцільно витрачати час на детальну оцінку. Експерти можуть зробити швидку оцінку, яка буде достатньою для планування та прийняття рішень;

при відсутності досвіду – якщо в компанії відсутня історія аналогічних проєктів, то методи, засновані на аналогіях, можуть бути непридатними. У цьому випадку експертна оцінка може бути єдиною доступною альтернативою;

при неузгодженості вимог – якщо вимоги до проєкту значно змінюються або є неузгодженими серед зацікавлених сторін, експерти можуть допомогти визначити можливий вплив цих факторів на вартість проєкту.

Відповідно до цього методу, особи, відповідальні за оцінку проєкту, можуть залучити додаткового фахівця, який проведе додаткову перевірку та уточнення оцінок. Рішення щодо необхідності залучення додаткового експерта до процесу оцінки вартості розробки ПЗ залежить від складності проєкту. Під час роботи над великими програмними рішеннями може знадобитися створити цілу команду технічних експертів і фахівців з конкретної області для допомоги в оцінці вартості проєкту.

Перевага в тому, що цей підхід є одним із найшвидших і простих у виконанні, і він не потребує значних ресурсів. Переважно його використовують на початкових етапах, коли мало доступних даних про проєкт [5].

Недоліком цього методу є те, що через новизну проєкту може виникнути складність у пошуку потрібного експерта. Крім того, іноді експерт може бути упередженим стосовно проєкту та допускати помилки. Також слід враховувати, що надійність оцінок може залежати від якості та об’єктивності експертного судження.

Метод референтних проєктів (Analogous Estimation)

Метод референтних проєктів або оцінка вартості на основі аналогії ґрунтується на аналізі схожих проєктів або їхніх частин для визначення вартості нового проєкту. Цей підхід використовує дані та параметри з попередніх подібних проєктів, щоб зрозуміти, скільки може коштувати розробка нового ПЗ. Іноді історичні дані можуть бути використані без змін для аналізу поточної роботи, а інколи їх потрібно скоригувати, враховуючи відмінності в обсязі або складності [6].

Оцінка складається з декількох етапів:

збір даних по проєкту, що розробляється;

відбір характеристик, за якими будуть порівнюватися проєкти;

пошук та аналіз проєктів, що є «аналогічними» розроблюваному;

експертна оцінка розроблюваного проєкту, в якій значення, запозичені з подібного проєкту, служать основою.

Зазвичай цей метод використовують у наступних ситуаціях:

відсутність інформації – коли немає досить деталізованої інформації про проєкт або коли проєкт є новим і немає історичних даних для порівняння;

наявність схожих проєктів – якщо є схожі проєкти, що вже завершилися і можуть бути використані для порівняння з поточним проєктом;

потреба в швидких результатах – коли необхідно швидко отримати приблизну оцінку вартості проєкту на ранньому етапі планування;

бюджетна обмеженість – у випадку обмеженого бюджету, коли немає можливості витратити багато коштів на докладний аналіз;

підтримка прийняття рішень – коли потрібно швидко визначити, чи варто розпочинати проєкт або які альтернативи варто розглянути.

Оцінка на основі аналогій може надати швидкі результати при низьких витратах, але такі результати не завжди є надійними. Крім того, вони сильно залежать від наявності подібних проєктів. Оцінка за допомогою цього методу зазвичай займає не більше кількох днів і використовується для приблизного розрахунку бюджету проєкту. Слід відзначити, що для

отримання точної аналогічної оцінки оцінювач повинен мати багаторічний досвід та значний портфель проєктів.

Метод функціональних точок (Function Point Analysis)

Метод функціональних точок базується на функціональних характеристиках ПЗ, він спроєктований для вимірювання функціональності, яку ПЗ надає користувачам. За допомогою цього методу можна оцінити вартість ПЗ на основі логічної моделі даних, а також на основі обсягу функціоналу, який вимагається від замовника і надається розробником [7].

Метод функціональних точок використовується для оцінки розробки на ранніх етапах проєкту, таких як логічне і концептуальне проєктування. Для використання цього методу потрібен перелік вимог до розроблюваного ПЗ. Точність оцінки залежить від рівня деталізації цих вимог [8].

Основні етапи методу функціональних точок під час оцінки вартості ПЗ містять:

визначення функціональних складових – на першому етапі ідентифікуються функціональні складові ПЗ, такі як введення даних, виведення інформації, запити користувачів, обробка даних тощо;

оцінка функціональних точок – для кожної функціональної складової обчислюються функціональні точки на основі певних розрахункових формул, які враховують кількість і складність функцій. Це дозволяє виміряти функціональну складність ПЗ;

визначення вагомості функціональних точок – кожна функціональна точка визначається вагомістю, яка вказує на важливість функції для користувача або бізнесу. Вагомість може бути високою, середньою або низькою залежно від важливості функції;

розрахунок функціональних балів – функціональні бали розраховуються як добуток кількості функціональних точок на їхню вагомість. Це дозволяє отримати загальну кількість функціональних балів для всього ПЗ;

визначення вартості на основі функціональних балів – за допомогою функціональних балів можна визначити вартість розробки, тестування і впровадження ПЗ. Цей розрахунок може містити витрати на робочий час, ресурси, інфраструктуру та інші фактори.

Цей метод дозволяє об’єктивно вимірювати функціональність ПЗ на основі конкретних характеристик, є відносно простим у розумінні та застосуванні, а також може бути використаний для оцінки ПЗ різної розмірності та складності. До недоліків можна віднести залежність від даних, які не завжди доступні на ранніх етапах та значні часові затрати на збір і аналіз вимог та розрахунки.

Метод «знизу-вгору» (Bottom-Up Estimation)

Даний метод оцінки вартості ПЗ полягає в розрахунку вартості проєкту на основі розгляду окремих компонентів, завдань або робіт, які складаються на найнижчому рівні деталей. Він передбачає розбиття проєкту на менші елементи та оцінку кожного елемента окремо, а потім сумування всіх цих оцінок для отримання загальної вартості проєкту. Цей підхід до оцінки витрат часто забезпечує високу точність. Однак отримання та агрегація цих деталізованих оцінок, як правило, вимагає певних ресурсів і може бути проблемою, особливо в великих або складних проєктах.

Алгоритм оцінки складається з таких етапів:

розбиття проєкту на менші компоненти або завдання, які можна оцінити окремо;

декомпозиція завдань на менші складові, доки вони не стануть достатньо дрібними для детальної оцінки;

експертна оцінка кожного елемента роботи залученими фахівцями або командою для проведення експертної оцінки;

сумування оцінок, отриманих для окремих компонентів або завдань (вартість, тривалість та інші важливі параметри);

додавання до оцінок часу, який потрібен для взаємодії між компонентами або завданнями, а також інші допоміжні витрати;

формування загального прогнозу вартості проєкту за допомогою суми всіх оцінок та додаткових витрат;

проведення контролю і корекції оцінок, якщо виникають зміни або ризики, що впливають на проєкт.

Перевагами методу «знизу-вгору» є висока точність та здатність враховувати усі деталі проєкту. Однак цей метод може бути часозатратним і вимагати більшого обсягу ресурсів для розробки детальної оцінки.

Метод параметричної оцінки (Parametric Estimation)

Цей метод оцінки вартості ПЗ використовує статистичний підхід для визначення очікуваних витрат або ресурсів на основі параметрів та значень, які мають взаємозв'язок зі створенням ПЗ. Цей метод передбачає використання математичних моделей або статистичних аналізів для оцінки витрат на розробку програми.

Основна ідея полягає в тому, що між різними параметрами проєкту (наприклад, розміром проєкту, складністю, кількістю функцій і т. ін.) та витратами на розробку ПЗ існує конкретна залежність, яку можна виразити у вигляді параметричної моделі. Параметрична оцінка може використовуватися в поєднанні зі складною статистичною або алгоритмічною моделлю, яка може враховувати багато кількісних і якісних параметрів для докладного регресійного аналізу.

Алгоритм оцінювання полягає в наступному:

збір вихідних даних про попередні проєкти або використання історичних даних зі схожих проєктів;

визначення параметричних моделей, які виражають залежність між параметрами проєкту та його вартістю. Ці моделі можуть бути математичними рівняннями або статистичними моделями;

калібрування моделей на основі зібраних даних. Містить підгонку моделей до історичних даних, щоб вони були точними;

застосування параметричних моделей до вхідних даних про новий проєкт, щоб прогнозувати витрати на його розробку;

оцінити точність прогнозу, порівнюючи результати з історичними даними або іншими методами оцінки;

проаналізувати прогнозовані витрати та їхні можливі варіації, а також врахувати фактори ризику та невизначеності;

після завершення оцінки підготувати звіт і розглянути його для прийняття рішення щодо вартості ПЗ та планування проєкту.

Як і в оцінці з аналогії, в параметричному методі використовуються раніше зібрані дані для отримання оцінок. Варто зазначити, що параметрична оцінка вимагає великих попередніх зусиль та часто розглядається як більш точніша альтернатива методу оцінки на основі аналогії. Проте для досягнення високого рівня точності потрібні додаткові ресурси для збору даних та проведення статистичного аналізу.

Підсумовуючи, можна сказати, що параметрична оцінка є швидким і вигідним методом, але точність залежить від якості даних. Якщо статистичні дані застаріли, то результати можуть бути недостатньо точними.

Порівняльний аналіз методів оцінки вартості ПЗ

Визначимо основні критерії, за якими буде відбуватися порівняння. Для наочності введемо рейтингову шкалу та оцінимо кожен критерій. При виборі оптимального методу опустимо дані про специфіку проєкту, доступність даних та обсяг робіт на ранніх етапах розробки, щоб можна було їх порівняти.

Перший критерій – це дані. Цей критерій використовується для порівняння якості та повноти даних, необхідних для кожного методу оцінки вартості ПЗ. Цей параметр неможливо оцінити за якоюсь шкалою, тому він буде використовуватися для проведення порівняльного аналізу в разі співпадіння балів, підрахованих на основі інших параметрів.

Другий критерій – це складність. Цей критерій показує, наскільки складно використовувати певний метод. Метод вважається простим у використанні, якщо за його допомогою можна провести оцінку вартості проєкту протягом розумного часу, і навпаки вважається складним, якщо він потребує використання складних формул та алгоритмів. Для цього критерію введемо шкалу від 1 до 3, де 1 бал – складний метод використання, 2 бали – середня складність використання і 3 бали – простий метод використання.

Третій критерій – універсальність. Універсальність – це здатність методу пристосовуватися до змін та відповідати різним технікам та стилям розробки. Введемо для нього шкалу оцінки від 1 до 3, де 3 бали будуть присвоєні методу оцінки, який підходить для будь-яких проєктів, 2 бали – методу, який потребує наявності певних специфічних умов для застосування, і 1 бал – методу, який підходить для обмеженої кількості проєктів.

Четвертий критерій – точність. Визначення точності полягає в тому, наскільки результат оцінки буде близьким до правильного значення. Введемо для нього шкалу оцінки від 1 до 3 балів, де 3 бали вказують на високу точність, 2 бали – середню точність і 1 бал – низьку точність оцінки вартості.

Отримані результати порівняльного аналізу наведені у таблиці 1.

Таблиця 1

Порівняльний аналіз методів оцінки витрат при розробці ПЗ

Метод	Дані	Складність	Універсальність	Точність
Експертна оцінка	Досвід та знання експертів	3	3	2
Оцінка по аналогії	Дані попередніх проєктів	3	2	1
Функціональні точки	Перелік вимог до ПЗ	2	3	3
«Знизу-Вгору»	Перелік вимог до ПЗ	1	1	3
Параметрична оцінка	Дані та параметри попередніх проєктів	2	2	2

З результатів порівняльного аналізу можна зробити висновок, що найбільш оптимальними методами для оцінки вартості ПЗ із розглянутих є методи експертної оцінки та функціональних точок, які набрали по 8 балів з 9 можливих. На відміну від експертної оцінки, метод функціональних точок не потребує залучення додаткових спеціалістів для проведення оцінки і є більш точним. Важливо також враховувати, що комбінація різних методів може забезпечити більш точну оцінку витрат та зменшити ризик помилок.

Висновки

Правильна оцінка вартості розробки ПЗ на початкових етапах проєктування є важливим етапом у забезпеченні успішності та ефективності реалізації будь-якого проєкту.

Експертні методи, такі як метод експертної оцінки й оцінка за аналогією, можуть бути швидкими і відносно дешевими, але їхні результати можуть бути менш точними і залежать від досвіду оцінювача.

Параметричні методи, такі як методи функціональних точок і параметричної оцінки, можуть забезпечити більш точні результати, але вони вимагають більше часу та ресурсів для підготовки і аналізу даних.

Метод «знизу-вгору» має високу точність та здатність враховувати усі деталі проєкту, але також вимагає багато часу та ресурсів.

У результаті порівняльного аналізу розглянутих в даній роботі методів було виявлено, що метод функціональних точок є найбільш гнучким та оптимальним для більшості проєктів. До його переваг можна віднести високу точність оцінки, масштабованість, відносну простоту

у використанні та придатність використання із проєктами різної ступені складності. На практиці вибір методу повинен залежати від конкретних умов і характеристик проєкту.

Перспективними **напрямками подальших наукових досліджень** є аналіз сучасних програмних рішень для оцінки вартості розробки ПЗ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Standish Group CHAOS Report // URL: https://www.standishgroup.com (дата звернення: 05.09.2023).

2. Сидоров Н. А., Баценко Д. В., Василенко Ю. Н., Щебетин Ю. В. Модели, методы и средства оценки стоимости программного обеспечения // Проблеми програмування. 2006. № 2. С. 290–298.

3. Лозовська Л. І., Дудник В. В. Сучасні підходи до вартісної оцінки програмних продуктів // Європейський вектор економічного розвитку. Економічні науки. 2014. № 2. С. 131–139.

4. Рябокінь Ю. М. Оцінка вартості програмного забезпечення // Вісник Київського національного університету технологій та дизайну. Серія: Технічні науки. 2015. № 1. С. 117–124.

5. Chirra S. M. R., Reza H. A Survey on Software Cost Estimation Techniques // Journal of Software Engineering and Applications. 2019. Т. 12. № 6. P. 226–248. URL: https://doi.org/10.4236/jsea.2019.126014 (дата звернення: 05.09.2023).

6. Rajeswari K., Beena R. A Critique on Software Cost Estimation // International Journal of Pure and Applied Mathematic. 2018. Т. 118. № 20. P. 3851–3862.

7. Nganga E., Tonui I. A Survey on Software Sizing for Project Estimation // International Journal of Software Engineering and Knowledge Engineering. 2015. Т. 5. № 4. P. 56–58.

8. Bundschuh, M., Dekkers, C. The IFPUG Function Point Counting Method // The IT Measurement Compendium. 2008. P. 323–363.

УДК 004.77

Кокошинський В. В. ORCID: 0000-0001-6364-6261 (ВІТІ ім. Героїв Крут)
Думітраш В. О. ORCID: 0000-0003-1996-3096 (ВІТІ ім. Героїв Крут)
Яковчук О. В. ORCID: 0000-0002-6312-5009 (ВІТІ ім. Героїв Крут)

ДОСЛІДЖЕННЯ ПЕРСПЕКТИВ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ SDN У ВІЙСЬКОВІЙ ТРАНСПОРТНІЙ ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ УКРАЇНИ

Вимоги до сучасних систем управління зв'язком суттєво посилились в останні роки, особливу актуальність це отримало з початком повномасштабного вторгнення рф в нашу державу. Системи управління повинні мати високу бойову готовність, пропускну здатність, стійкість, мобільність, доступність, розвідувальну захищеність, керованість та забезпечувати виконання вимог щодо своєчасності, достовірності та безпеки інформаційного обміну. Тому впровадження новітніх технологій, особливо з утворенням єдиного інформаційного простору за допомогою переходу на єдину технологічну платформу для різнорідних підсистем зв'язку, здатні значно покращити рівень виконання даних вимог. Однією з таких технологій є мережева платформа SDN, в якій площина керування відокремлена від площини даних та застосувань. Ідея впровадження даної технології досліджувалась вітчизняними фахівцями, втім, не було запропоновано механізму для комплексного застосування технології SDN у вітчизняній системі управління зв'язку, зокрема в військовій транспортній телекомунікаційній мережі.

У цій статті ми представляємо підхід на основі програмно-конфігурованої мережі (SDN) для створення перспективної військової транспортної телекомунікаційної мережі на базі існуючої. Цей підхід пропонує декілька можливостей, у тому числі поетапний перехід різнорідних мереж, що входять до складу військової транспортної телекомунікаційної мережі та її управління як гібридною гетерогенною мережею з внутрішньосмуговим керуванням на основі відкритої мережевої операційної системи ONOS з використанням протоколу ieHDDP. У статті також пропонуються подальші кроки з побудови математичної моделі перспективної військової транспортної телекомунікаційної мережі та її дослідження. У майбутньому також планується дослідження перспективних вдосконалень моделі, зокрема, таких як можливість впровадження хмарного континууму.

Ключові слова: *програмно-конфігурована мережа SDN, військова транспортна телекомунікаційна мережа, ONOS, гібридна мережа, внутрішньосмугове керування.*

V. Kokoshynsky, V. Dumitrash, O. Yakovchuk Study of the prospects for the use of SDN technology in the military transport telecommunication network of Ukraine.

The requirements for modern communication management systems have significantly increased in recent years, and this became particularly relevant with the beginning of the full-scale invasion of the Russian Federation into our country. Control systems must have high combat readiness, throughput, stability, mobility, availability, intelligence security, manageability, and ensure compliance with requirements for timeliness, reliability and security of information exchange. Therefore, the introduction of the latest technologies, especially with the formation of a single information space through the transition to a single technological platform for heterogeneous communication subsystems, can significantly improve the level of fulfillment of these requirements. One such technology is the SDN network platform, in which the control plane is separated from the data and application planes. The idea of introducing this technology was studied by domestic specialists, however, no mechanism was proposed for the comprehensive application of SDN technology in the domestic communication management system, in particular in the military transport telecommunication network.

In this article, we present a software-defined network (SDN)-based approach to build a promising military transport telecommunications network based on an existing one. This approach offers several possibilities, including the phased transition of the heterogeneous networks that make up the military transport telecommunications network and its management as a hybrid heterogeneous network with in-band control based on the ONOS open network operating system using the ieHDDP protocol. The article also suggests further steps in building a mathematical model of a prospective military transport telecommunication network and its research. In the future, it is also planned to study promising improvements of the model, in particular, such as the possibility of introducing a cloud continuum.

Keywords: *software-configurable SDN network, military transport telecommunication network, ONOS, hybrid network, in-band management.*

Постановка проблеми. Діяльність Збройних сил України, особливо під час ведення активних бойових дій, характеризується специфічними, особливо суворими вимогами до інформації і до засобів зв'язку та передавання даних.

Аналіз сучасного світового досвіду свідчить, що успішне проведення військових операцій вимагає своєчасного комплексного інформаційного забезпечення бойових дій, що вже неможливе без сучасних інформаційних технологій. Сьогодні наслідки неефективної роботи з інформацією – це втрати особового складу, озброєння та військової техніки, які значною мірою зумовлюють перемогу або поразку. При цьому постає необхідність вдосконалення управління, підвищуються вимоги до показників якості та надійності системи управління інформаційно-телекомунікаційними мережами, особливо в кризових ситуаціях.

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 усіма видами інформації між органами й пунктами управління (всіх ланок) з відповідною своєчасністю, достовірністю і безпекою [1].

Важлива роль щодо вдосконалення відводиться впровадженню новітніх технологій для здійснення якісного управління системою військового зв'язку (далі – СВЗ), зокрема, військовою телекомунікаційною системою, що являє собою сукупність військових телекомунікаційних мереж доступу та військової транспортної телекомунікаційної мережі і призначена для забезпечення службових осіб органів військового управління телекомунікаційними послугами та надання каналів передавання і групових трактів.

Одним із перспективних напрямків досліджень є вивчення перспектив впровадження технології SDN у вітчизняній СВЗ та ефекту покращення кількісних та якісних характеристик зв'язку від її впровадження. Це питання досліджувалось багатьма вітчизняними фахівцями, втім, наразі існує низка невирішених питань щодо глобального застосування технології SDN у військовій транспортній телекомунікаційній мережі (далі – ВТТМ).

Постає наукове завдання щодо дослідження підвищення ефективності зв'язку при застосуванні технології SDN, зокрема її вплив на пропускну здатність, захищеність, мобільність та масштабованість перспективної ВТТМ.

Аналіз останніх досліджень і публікацій

Серед основних задач щодо перспектив застосування технології SDN у вітчизняній ВТТМ розглядались наступні наукові задачі:

обмеження та перерозподіл навантаження в SDN мережах [2], автор пропонує алгоритм оптимізації завантаженості серверів SDN, однак не розглядає питання автоматизації рішення цієї задачі;

актуальність архітектури SDN мереж та проблема забезпечення якості їх обслуговування розкриті в роботі [3], проте, авторами не пропонується конкретний алгоритм розв'язання задачі;

аналіз методів багатошляхової маршрутизації у SDN мережах розглянуто в роботі [4], висвітлюються переваги впровадження та використання цих методів, але не наводяться приклади їх практичної реалізації в мережах або моделі їх подальшого впровадження.

Серед іноземних фахівців задачі, пов'язані з застосуванням SDN у військових ТКМ, розглядались зокрема у роботі [5]. Авторами пропонується модель побудови військової ТКМ з використанням хмарного континууму або концепції «обчислення на вимогу» (On-demand computing –ODC) та адаптації інших сучасних технологій, які знайшли поширення в цивільних галузях до військових потреб, наприклад, Інтернет військових речей (IoMT) та інші. Одночасно виникає нагальна потреба адаптувати такий досвід світової спільноти для впровадження у вітчизняних ТКМ.

Отже, в наведених статтях не повною мірою були висвітлені наукові задачі поетапного переходу гетерогенної ВТТМ на платформу SDN, подальшого функціонування та підвищення ефективності СВЗ завдяки застосуванню технології SDN.

Мета статті – дослідження наукової задачі вивчення ефективності та здобутків від поетапного впровадження технології SDN для вітчизняної перспективної ВТТМ та наукове обґрунтування для застосування технології SDN, її функціонування та керування в межах СВЗ.

Виклад основного матеріалу дослідження. Військовий зв'язок є основним засобом управління військами, бойовими засобами та зброєю та виконує завдання по обміну інформацією в системах управління військами. Серед основних вимог та характеристик СВЗ слід виділити: цілісність, достовірність, своєчасність, скритність та пропускну здатність.

Цілісність забезпечується узгодженістю протоколів взаємодії та сумісністю інтерфейсів технічних засобів телекомунікацій.

Достовірність – здатність військового зв'язку забезпечувати відтворення інформації з заданою точністю при її обміні та обробці.

Своєчасність – здатність військового зв'язку забезпечувати обмін інформацією, її обробку та рішення інформаційних і розрахункових задач у задані (нормативні) строки.

Скритність – здатність військового зв'язку зберігати в таємниці факт передачі та зміст інформації при її обміні, обробці, зберіганні та вирішенні інформаційних і розрахункових задач.

Пропускна здатність визначає потенційні можливості військового зв'язку щодо об'єму інформації, який можна передати/отримати каналами зв'язку за одиницю часу.

СВЗ має стаціонарний та мобільний компоненти, системи (мережі) різного призначення.

ВТТМ – частина СВЗ, що призначена для забезпечення службових осіб органів військового управління каналами передавання і груповими трактами. Це мережа, що забезпечує передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду між підключеними до неї телекомунікаційними мережами доступу, та до складу якої входять прямі телекомунікаційні лінії (мережі), опорна телекомунікаційна мережа, орендовані канали передавання і групові тракти (рис. 1).

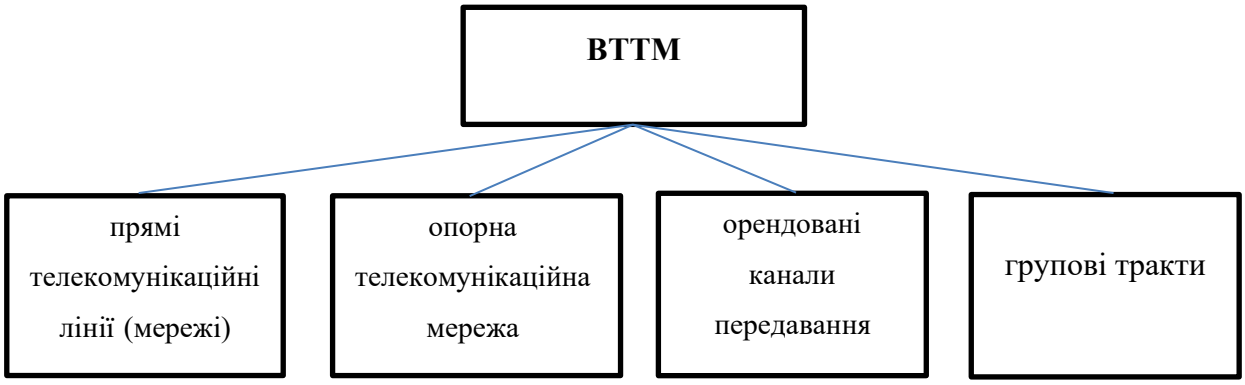

Рис. 1. Складові ВТТМ

До перспективної ВТТМ висуваються такі вимоги:

ВТТМ має забезпечувати виконання функцій передачі інформації в інтересах органів військового управління ЗС України, МО України;

ВТТМ повинна бути масштабованою, адаптованою, захищеною та стійкою.

ВТТМ повинна вирішувати такі завдання:

забезпечення гарантованого обміну інформацією в межах стаціонарної системи зв'язку та польової мережі зв'язку;

безвідмовного функціонування, незважаючи на наявність ймовірних помилок (дефектів), які можуть проявлятися під час експлуатації.

Ключова відмінність між SDN і традиційною мережею полягає в інфраструктурі: традиційна мережа базується на апаратному забезпеченні, тоді як SDN базується на

програмному забезпеченні, що робить її набагато гнучкішою, ніж традиційна мережа. Це дозволяє адміністраторам контролювати мережу, змінювати параметри конфігурації, надавати ресурси та збільшувати пропускну здатність мережі – все це через централізований інтерфейс користувача без використання додаткового обладнання (рис. 2).

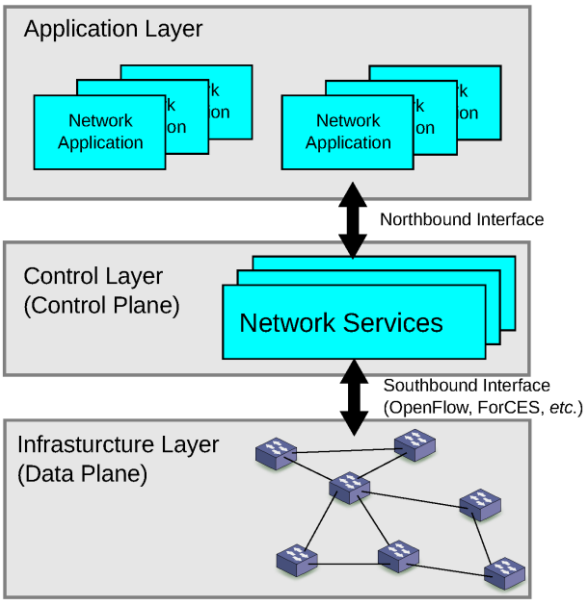

Рис. 2. Мережева архітектура SDN

У цьому контексті SDN є багатообіцяючим підходом для управління складною та неоднорідною мережевою інфраструктурою, якою є, зокрема, ВТТМ.

Первісний проєкт площини керування SDN використовував лише один контролер для мережі. Незважаючи на переваги централізованого керування мережею SDN, наявність лише одного контролера було проблемою через обмежену потужність єдиного контролера та як єдина точка відмови мережі SDN, оскільки несправність контролера призводила до розриву зв'язку між контролером та комутаторами.

Для вирішення зазначеної проблеми було запропоновано побудову площини керування SDN на основі декількох контролерів або мультиконтролера.

Серед основних проблемних питань, пов'язаних з використанням мультиконтролера у SDN, виділяються: масштабованість, послідовність, надійність і балансування навантаження [10]. Дотримуючись логіки проєктування, автори досліджували масштабованість мультиконтролера для вирішення проблеми одного контролера (єдина точка відмови, обмежені ресурси керування тощо), а також проводили дослідження послідовності, надійності та балансування навантаження, спричинені кількома контролерами.

Одним із найбільш потужних розподілених контролерів SDN є ONOS (Open Network Operating System). Він забезпечує площину керування SDN, розподіляючи її на гнучкі сегменти та роботу програмних модулів для відповідного адміністрування всієї мережі.

Операційна система ONOS була розроблена як платформа для створення рішень операторського рівня, які використовують переваги апаратного забезпечення «білих скриньок», пропонуючи при цьому гнучкість для створення та розгортання нових динамічних мережевих служб із спрощеними програмними інтерфейсами. ONOS підтримує як конфігурацію, так і керування мережею в реальному часі, усуваючи необхідність запускати протоколи керування маршрутизацією та комутацією всередині мережевої структури. Завдяки перенесенню інтелекту в хмарний контролер, ONOS відкрита для впровадження інновацій,

і в ній легко створювати нові мережеві програми без необхідності змінювати системи площини даних.

Для побудови перспективної ВТТМ пропонується використання платформи ONOS, що є провідним контролером SDN із відкритим кодом для створення поглиблених рішень SDN для складових ВТТМ.

Платформа ONOS містить:

платформу та набір додатків, які діють як поширений модульний розподілений контролер SDN;

спрощене керування конфігурування та розгортання нового програмного забезпечення, обладнання та послуг;

масштабовану архітектуру для забезпечення стійкості та масштабованості, необхідних для відповідності суворим умовам середовища ВТТМ.

Для здійснення управління перспективною ВТТМ пропонується здійснювати розгортання площини керування SDN так, що площина керування та дані спільно використовують ту саму фізичну мережу, що покращує гнучкість мережі та можливість її програмування, знижує витрати та підвищує надійність мережі.

Ця концепція називається внутрішньосмуговим керуванням та може бути легше реалізована в існуючій транспортній мережі наявної СВЗ при переході на технологію SDN.

Разом з тим, при внутрішньосмуговому керуванні виникає кілька проблем, таких як вразливість безпеки, перевантаження мережі та втрата даних. У літературі описані різноманітні конструкції внутрішньосмугового керування для покращення роботи мереж SDN [6–9]. У цих документах розглядаються різні підходи, запропоновані нині для вдосконалення внутрішньосмугового керування SDN на основі чотирьох основних категорій: автоматична маршрутизація, швидке відновлення після збою, завантаження мережі та розподілене керування.

ВТТМ складається з різнорідних складових, в частині з яких технологія SDN може бути впроваджена раніше, а в інших – через деякий проміжок часу або зовсім не бути впроваджена (як, наприклад, в орендованих каналах). Тому, для її безперебійної та якісної роботи пропонується використання протоколу виявлення HDDP для гібридних мереж [7] та його вдосконаленої версії ieHDDP [8].

Авторами [7] було запропоновано протокол виявлення – Hybrid Domain Discovery Protocol (HDDP), який покращував існуючий на той час OpenFlow Discovery Protocol (OFDP). HDDP дозволяв виявляти гібридні мережеві топології, що складались як з пристроїв SDN, так і тих, що не підтримують SDN. HDDP було реалізовано в програмному комутаторі та емульовано в різноманітних мережах, де він виявляв гібридні топології за допомогою ряду повідомлень.

Наступним кроком фахівцями [9] було розроблено протокол eHDDP, який не тільки був здатний виявляти гібридні топології SDN як з пристроями SDN, так і не-SDN, а також міг мати справу з дротовим та бездротовим обладнанням. Це дозволило інтегрувати всю інформацію з рівня 2 у площину керування SDN, включаючи пристрої як з дротовими, так і з бездротовими інтерфейсами. Отже, протокол eHDDP не тільки дозволяв керувати складною базовою мережею, але навіть збирати інформацію з бездротових мереж, підключених до дротової інфраструктури. Окрім цього, інформація, зібрана з рівня інфраструктури, дозволяла розрізняти двонаправлені та однонаправлені бездротові канали зв’язку, що було корисним для оптимізації зв’язку в бездротових мережах.

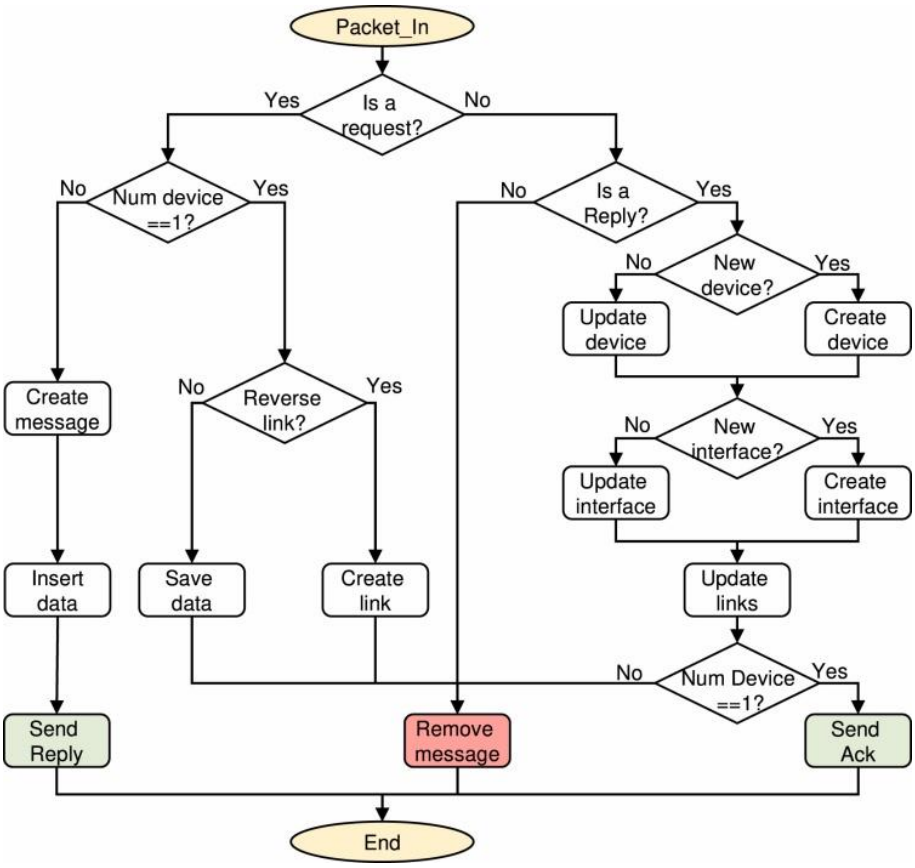

Рис. 3. Програма контролера eHDDP

Площина керування SDN повинна реалізовувати логіку, узагальнену на рисунку 3, для обробки топологічної інформації, що передається керуючими повідомленнями eHDDP із площини даних. Ця логіка була реалізована в програмі контролера відкритої мережевої операційної системи (ONOS) і використовує протокол OpenFlow для зв'язку між пристроєм і контролером SDN. Контролер відповідає за початок процесу дослідження, надсилаючи стільки повідомлень Request через Packet-Out, скільки SDN-пристроїв було раніше виявлено агентом OpenFlow [9].

Протокол запускався площиною керування та працював у дві фази. Спочатку він досліджував базову мережу за допомогою повідомлення про відкриття, яке транслювалось з площини керування, а потім передавав топологічну інформацію, отриману мережевими пристроями під час фази дослідження, назад до площини керування.

Протокол ieHDDP [8], який є вдосконаленням eHDDP, не лише передає топологічну інформацію, а також здатний встановлювати внутрішньосмугові канали керування в гібридних доменах SDN, у яких співіснують SDN/не-SDN та дротові/бездротові пристрої. Встановлення внутрішньосмугового каналу керування базується на дослідницькому процесі, ініційованому площиною керування, який охоплює всі пристрої за допомогою механізму контрольованого затоплення, що дозволяє виявити порт/наступний стрибок для встановлення шляху від кожного пристрою до контролера(ів) SDN), і водночас він запам'ятовує всю необхідну топологічну інформацію. Цей шлях дозволяє пристроям SDN встановлювати з'єднання з площиною керування SDN.

Рішення ieHDDP порушує традиційне припущення, згідно з яким площина даних повністю залежить від площини керування. Причиною цього порушення є симетрія, запроваджена ieHDDP, яка полягає у збалансованій координації між площинами даних і керування. Площина даних вимагає, щоб площина керування мала відповідну конфігурацію,

тоді як площина керування вимагає, щоб площина даних отримувала внутрішньосмуговий канал керування, що є ключовим у гібридних гетерогенних мережах, де вихідний канал керування для всіх пристроїв неможливий. Отже, ieHDDP заповнює прогалину, знаходячи інтегроване рішення, яке виконує обидві задачі (виявлення топології та налаштування внутрішньосмугового каналу керування) одночасно в гібридних середовищах SDN.

У сценарії ieHDDP пристрої SDN є резервними вузлами; вони не можуть підключитися до площини керування, оскільки їм бракує необхідних знань (порту контролера та, можливо, навіть мережевої адреси площини керування), поки їх не розбудить повідомлення дослідження служби виявлення. Однак впровадження попереднього eHDDP у пристроях SDN дозволить їм дізнатися шлях до контролера шляхом встановлення порту контролера, щоб досягти площини керування. На жаль, цього недостатньо для встановлення внутрішньосмугового каналу керування, оскільки eHDDP сам по собі не забезпечує підтримку зв'язку у зворотному напрямку, від площини керування до мережевих пристроїв.

Отже, відповідно до розробки авторів [8], робота сценарію ieHDDP тепер буде складатись з чотирьох фаз (рис. 4).

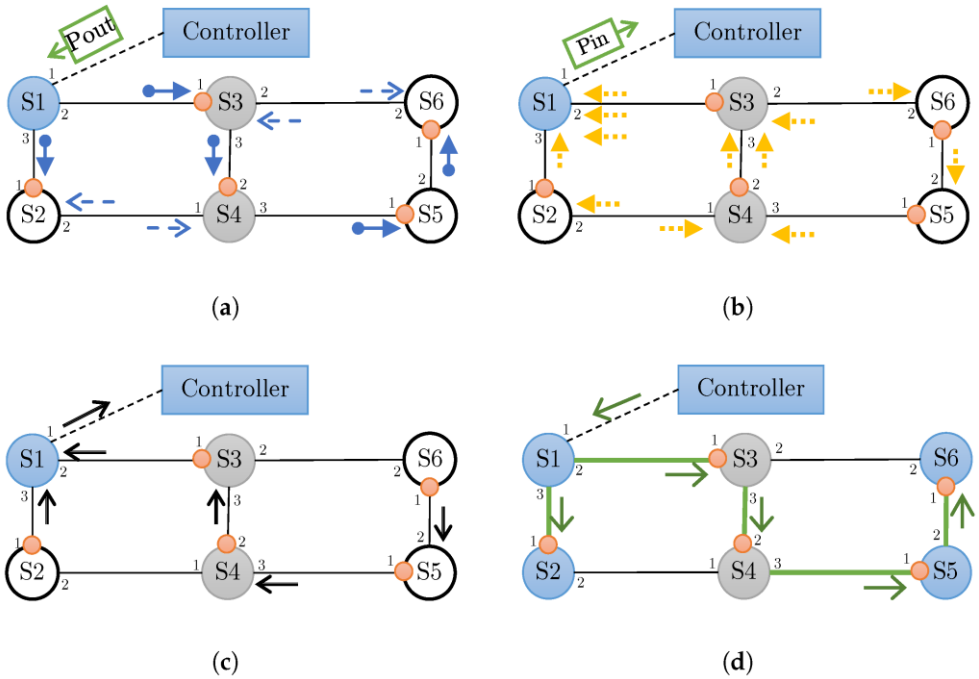

Рис. 4. Приклад створення внутрішньосмугового каналу в ieHDDP: *a* – фаза дослідження мережі; *b* – фаза підтвердження; *c* – фаза внутрішньосмугового навчання каналу; *d* – фаза підтвердження внутрішньосмугового каналу

1. Фаза дослідження (навчання порту контролера).

Фаза дослідження мережі ieHDDP (яка схожа на вихідну фазу в eHDDP) показана на рис. 4, *a*. Його запускає площина керування SDN шляхом передачі повідомлення ieHDDP Request у мережу через *S*1, як пояснюється в [9]. Вхідний порт першої копії, отриманої на кожному комутаторі, заблоковано, що запобігає пересиланню комутатором запізнілих копій того самого повідомлення ieHDDP Request, отриманого на інших портах, щоб уникнути петель. Потім заблокований порт позначається як порт контролера в кожному вузлі, за винятком тих, які вже підключені до площини керування (лише *S*1 у нашому прикладі), що також запускає фазу внутрішньосмугового навчання каналу.

2. Фаза підтвердження (збір топологічної інформації).

Ця фаза залишається незмінною. Вона працює так само, як і в eHDDP (рис. 4, *b*). Кожного разу, коли пізню копію отримує вузол, генерується повідомлення ieHDDP Reply , яке

надсилається назад через вхідний порт пізньої копії. Кожен комутатор, який отримує повідомлення ieHDDP Reply, оновлюватиме свій вміст, щоб включити себе в маршрут перед тим, як передавати його на площину керування через порт контролера. Нарешті, коли повідомлення ieHDDP Reply надходить на *S*1, який підключено до контрольної площини, воно надсилається безпосередньо до нього через відповідне повідомлення PacketIn без подальшої обробки.

3. Фаза навчання внутрішньосмугового каналу.

Разом із наступною фазою процес, показаний на рис. 4, *c*, реалізує базовий навчальний перемикач у кожному комбінованому пристрої SDN/ieHDDP, щоб можна було вивчити двонаправлений шлях до площини керування. Він запускається, коли порт, заблокований першою копією, отриманою з повідомлення запиту ieHDDP, позначається як порт контролера на *S*2, *S*5 та *S*6. Щоб налаштувати з'єднання з площиною керування, вони надсилають лише через порт контролера повідомлення ARP Request, шукаючи MAC-адресу площини керування. Кожен проміжний вузол оброблятиме повідомлення запиту ARP і зберігатиме кортеж <MAC-адреса джерела, вхідний порт> у таблицю навчання, перш ніж передавати повідомлення через власний порт контролера до рівня керування. Нарешті, коли повідомлення запиту ARP надходить на *S*1, воно обробляється так само, а потім надсилається безпосередньо на сервер, на якому працює площина керування. У нашому прикладі після повної обробки повідомлень ARP-запиту від *S*2, *S*5 і *S*6 в мережі було визначено односпрямований шлях, що охоплює *S*1 до будь-якого з них. Ці шляхи стануть двонаправленими після підтвердження внутрішньосмугового каналу та останньої фази.

4. Фаза підтвердження внутрішньосмугового каналу (навчання MAC контролера).

Після отримання повідомлення запиту ARP сервер, на якому запущена площина керування, видає відповідну відповідь ARP. *S*1 уже знає, як досягти вузла призначення ARP-відповіді (*S*2, *S*5 або *S*6), вони зберігаються в його таблиці навчання (рис. 4, *d*), тому він просто пересилає ARP-відповідь до місця призначення. Тепер проміжні вузли на шляху оброблять відповідь ARP і оновлять свою відповідну таблицю навчання новим записом, що вказує на площину керування, кортеж <MAC-адреса джерела відповіді, вхідний порт>, перш ніж передавати його наступному комутатору на шляху. Так кожен комутатор, відвіданий ARP-відповіддю, дізнається як дістатися до контрольної площини, двонаправлено перетворюючи шлях до відповідного комутатора призначення. Нарешті, двонаправлені шляхи від *S*2, *S*5 та *S*6 до площини керування будуть на місці, а внутрішньосмугові з'єднання можна налаштувати так, щоб ці комутатори стали з'єднаними (вони змінюють колір з білого на синій на рис. 4, *d*); це означає, що вони можуть встановлювати з'єднання з площиною керування, як очікувалося, подібно до пристроїв SDN, оскільки внутрішньосмуговий канал керування вже встановлено та функціонує.

Площина управління повинна періодично запускати всі попередні фази, виконуючи початкову фазу дослідження. Ця періодичність гарантує як виявлення змін топології, так і відновлення внутрішньосмугового каналу керування у разі збоїв [8].

Використання вищезазначеного контролера та протоколів виявлення гібридних мережевих топологій пропонується для забезпечення якісного рівня зв'язку в такій гетерогенній системі, якою є перспективна ВТТМ.

Для проведення подальшого дослідження ефективності поетапного впровадження технології SDN у вітчизняну ВТТМ пропонується побудувати її деталізовану математичну модель з емулюванням процесів, які в ній відбуваються, на платформі Mininet або аналогічній з можливістю відтворення мереж різних типів.

Для оцінки ефективності – провести порівняльний аналіз роботи моделі мережі, побудованої за допомогою традиційної архітектури та при поетапному введенні в мережу елементів з застосуванням архітектури SDN. Змінюючи кількість вузлів та топології кожної з мереж, провести серію випробувань моделі.

Надалі скласти таблицю оцінки ефективності для кожної мережі, яку ми досліджуємо Z_1, …, Z_J розрахувати та порівняти Z_j для кожної мережі.

Використовуючи критерії оцінки ефективності K_i та ваг W_{ij} для розрахунку Z_j кожної j-ї мережі знайти мережу з найкращою ефективністю для j-мереж Z_j за формулою (1):

$$\max_j Z_j = \frac{\sum_{i=1}^{I} W_{ij}}{i}, \quad (1)$$

де $i=\overline{1,I}, j = \overline{1,J}$;

i – поточний критерій;

j – поточний номер мережі;

I – загальна кількість критеріїв;

J – загальна кількість досліджуваних варіантів побудови мереж;

W_{ij} – вага критерію K_i;

Z_j – оцінка j-ї мережі.

За результатами отриманих результатів провести аналіз.

В якості критеріїв та основних досліджуваних мереж можна взяти дані, наведені в таблиці 1.

Таблиця 1

Порівняльна оцінка ефективності традиційних мереж та мережі SDN

Тип мережі / Критерій оцінки	Традиційна мережа (архітектура 1)	Традиційна мережа (архітектура 2)	SDN мережа
Цілісність	0,3	0,4	0,8
Своєчасність	0,6	0,5	0,7
Достовірність	0,5	0,6	0,7
Скритність	0,4	0,5	0,6
Пропускна здатність	0,3	0,5	0,6
Вартість впровадження	0,9	0,8	0,3
Оцінка ефективності моделі (Z_j)	**0,5**	**0,55**	**0,62**

Отримані дані можна зобразити за допомогою діаграми (рис. 5).

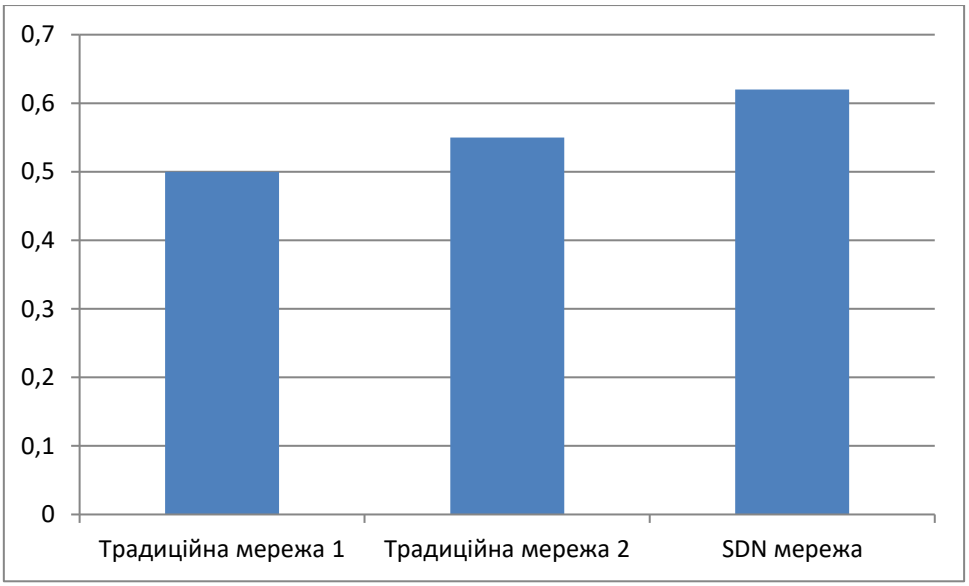

Рис. 5. Діаграма оцінки ефективності моделі

Тоді формула (1) прийме вигляд (2):

$$\max_j Z_j = \frac{\sum_{i=1}^{6} w_{ij}}{6}, \quad (2)$$

де $i=\overline{1,6},\ j=\overline{1,2}$.

Виходячи з максимального значення Z_j, можна приймати рішення щодо доцільності впровадження SDN технологій у перспективній ВТТМ.

Висновки. У цій статті була вирішена наукова задача щодо обґрунтування доцільності побудови перспективної ВТТМ на базі технології SDN із використанням світового досвіду та останніх розробок фахівців, які дозволяють врахувати особливості існуючої вітчизняної мережі та її складових. Запропонована перспективна ВТТМ може бути впроваджена у вигляді гібридної гетерогенної мережі з внутрішньосмуговим керуванням на основі відкритої мережевої операційної системи ONOS з використанням протоколу ieHDDP для якісного управління різнорідних складових у єдиній ВТТМ. Також було запропоновано спосіб побудови математичної моделі перспективної ВТТМ та її дослідження з проведенням оцінки критеріїв ефективності та порівняльного аналізу таких характеристик, як пропускна здатність, захищеність, мобільність та масштабованість існуючої та перспективної ВТТМ.

Перспективи подальших досліджень. У майбутньому планується побудова деталізованої математичної моделі перспективної вітчизняної ВТТМ та проведення експериментів з емулюванням гібридних топологій включно з дротовими/бездротовими та SDN/не-SDN пристроями. А також дослідження перспективних вдосконалень, зокрема, таких як можливість впровадження хмарного континууму для зниження часу затримки та посилення безпеки у вітчизняній ВТТМ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Шолудько В. Г., Остапчук В. М., Ольшанський В. В., Пивоварчук С. А., Стойчев М. І., Філіпов В. В. Організація військового зв’язку: навч. посіб. Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 2021. 259 с.

2. Бовда Е. М. Алгоритм управління балансуванням навантаження в SDN мережах // Збірник наукових праць ВІТІ. 2018. № 4. С. 14–20.

3. Єфанова К. О., Пономаренко З. М., Масесов М. О. Актуальність впровадження та використання мережі SDN // Сучасні інформаційні технології у сфері безпеки та оборони. 2018. № 2. С. 147–150. URL: http://nbuv.gov.ua/UJRN/sitsbo_2018_2_25.

4. Симоненко О. А., Троцько О. О., Кушніренко Д. М. Аналіз методів багатошляхової маршрутизації в програмно-конфігурованих телекомунікаційних мережах // Збірник наукових праць ВІТІ. 2019. № 2. С. 95–104.

5. E. Rojas, D. Lopez-Pajares, J. Alvarez-Horcajo, S. Llopis Sánchez. The Cloud Continuum for Military Deployable Networks: Challenges and Opportunities // Computer Security. ESORICS 2022 International Workshops: CyberICPS 2022.

6. Carrascal D., Rojas E., Arco J. M., Lopez-Pajares D., Alvarez-Horcajo J., Carral J. A. A Comprehensive Survey of In-Band Control in SDN: Challenges and Opportunities. Electronics. 2023. № 12 (6). 1265 p. URL: https://doi.org/10.3390/electronics12061265.

7. J. Alvarez-Horcajo, E. Rojas, I. Martinez-Yelmo, M. Savi and D. Lopez-Pajares, "HDDP: Hybrid Domain Discovery Protocol for Heterogeneous Devices in SDN", in IEEE Communications Letters, vol. 24, вип. 8, стор. 1655-1659, серпень 2020 р. URL: doi: 10.1109/LCOMM.2020.2991347.

8. Alvarez-Horcajo J., Martinez-Yelmo I., Rojas E., Carral J. A., Carrascal D. ieHDDP: An Integrated Solution for Topology Discovery and Automatic In-Band Control Channel Establishment for Hybrid SDN Environments. Symmetry 2022, 14, 756. URL: https://doi.org/10.3390/sym14040756.

9. T.-S. Wong and S. S. W. Lee, "Design of an In-Band Control Plane for Automatic Bootstrapping and Fast Failure Recovery in P4 Networks," in IEEE Transactions on Network and Service Management, URL: https:// doi.org/10.1109/TNSM.2023.3242222.

10. T. Hu, Z. Guo, P. Yi, T. Baker and J. Lan, "Multi-controller Based Software-Defined Networking: A Survey," in IEEE Access, vol. 6, pp. 15980-15996, 2018, URL: https://doi.org/10.1109/ ACCESS.2018.2814738.

УДК 004.93

Куцаєв В. В. ORCID: 0000-0001-8213-4739 (ВІТІ ім. Героїв Крут)
Лазута Р. Г. ORCID: 0000-0002-8584-1110 (ВІТІ ім. Героїв Крут)
Головко О. Є. ORCID: 0009-0002-7549-8125 (ВІТІ ім. Героїв Крут)

ОБРИС ПОШИРЕНОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МОДЕЛІ НЕЙРОНА

Суть статті полягає в дослідженні додаткових можливостей біологічного нейрона відповідно до припущень авторів. Припущення надають можливість запропонувати поширену математичну модель нейрона та провести початкові дослідження принципів і можливостей телекомунікаційної обробки інформації, які виникають завдяки реалізації припущення авторів, позичених у живих нейронах головного мозку людини.

Припущення авторів щодо поширення можливостей нейрона базовано на багатошаровості ядра нейрона. Автори припускають, що окремі шари ядра нейрона здатні зберігати сліди пам'яті, зафіксовані у різні періоди часу функціонування нейрона. Також зроблено припущення про те, що кожний нейрон є часткою ансамблю, який відповідає за одну з функцій одного з видів почуттів людини, а саме: зору, слуху, смаку, нюху, дотику, болю та температури. При цьому цей нейрон взаємопов'язаний одним періодом часу з групами нейронів всіх інших ансамблів, відповідальних за всі інші почуття.

Автори вважають що таке переплетіння формує принцип мотивації та емоцій у головному мозку людини та надає величезні переваги в механізмі навчання нейронних ансамблів і механізмі розпізнавання інформації. Автори вважають, що схожа схема властива живим нейронним ансамблям. Таке переплетіння нейронів та спеціалізація груп нейронів відсутні в штучних мережах, тому в них немає природньої надлишковості, мотивації, в них не задіяні всі механізми обробки інформації, які використовує головний мозок людини.

Автори передбачають, що кожний нейрон із групи нейронів одного з видів почуттів або спеціалізованого функціонального ансамблю здатен віддавати сліди інформації, зафіксовані ним у різні відрізки часу, а також збуджувати інші пов'язані з ним у часі нейрони з груп іншого виду почуттів або спеціалізованого функціонального ансамблю.

Автори намагались описати математичну та схематичну моделі штучного нейрона відповідно до свого припущення. Подальші шляхи досліджень можуть торкатися таких напрямків: опис алгоритму роботи спрощеної мережі, створеної з одиноких штучних нейронів, пов'язаних між собою згідно з припущенням авторів; опис роботи мережі, складеної з шарів нейронів, навчених за одним із періодів часу існування штучного нейрона; опис роботи мережі, складеної з шарів нейронів різних видів почуттів або функціональних ансамблів; опис роботи окремої мережі, яка фіксує схеми зв'язків запропонованих вище мереж.

Ключові слова: *головний мозок людини, нейрон, штучна мережа, сліди інформації.*

V. Kutsaiev, R. Lazuta, O. Golovko Outline of a common telecommunication model of a neuron.

The essence of the article is the study of additional capabilities of the biological neuron in accordance with the authors' assumptions. The assumptions provide an opportunity to propose a common mathematical model of a neuron and to conduct initial research into the principles and possibilities of telecommunication information processing, which arise due to the implementation of the authors' assumptions borrowed from living neurons of the human brain.

The authors' assumption regarding the spread of the neuron's capabilities is based on the multi-layered nature of the neuron's core: the authors assume that individual layers of the neuron's core are able to store memory traces recorded in different time periods of the neuron's functioning. It is also assumed that each neuron is a part of an ensemble that is responsible for one of the functions of one of the types of human senses, namely: vision, hearing, taste, smell, touch, pain, and temperature. At the same time, this neuron is interconnected with groups of neurons, respectively, of all other ensembles responsible for all other senses.

The authors believe that such an interweaving forms the principle of motivation and emotions in the human brain and provides enormous advantages in the mechanism of learning neural ensembles and the mechanism of information recognition. The authors believe that a similar scheme is suitable for living neural ensembles. This interweaving of neurons and specialization of groups of neurons are absent in artificial networks, therefore they do not have natural excess motivation and all information processing mechanisms used by the human brain are not involved.

The authors predict that each neuron from a group of neurons of one of the types of senses or a specialized functional ensemble is capable of giving traces of information recorded by it at different time intervals, as well as wakes up another neuron related to it in time from a group of another type of senses or a specialized ensemble.

The authors tried to describe the mathematical and schematic model of an artificial neuron according to the authors' assumption.

Further ways of research can concern the next directions: description of the algorithm of operation of a simplified network created from single artificial neurons which connected between each other according to author's assumptions; description of the operation of a network composed of layers of neurons trained for one of the periods of the artificial

neuron's existence; operation description of a network, that is composed of layers of neurons of various senses types or functional ensembles description of the operation of a separate network, which fixes the connection schemes of the networks proposed above.

Keywords: *human brain, neuron, artificial network, traces of information.*

Постановка завдання в загальному вигляді. Сучасна війна має яскраво виражений мережецентричний інформаційно-технічний характер. Перемога над лютим ворогом залежить від переваги над противником за всіма військовими компонентами [1]. Автори вважають, що дуже важливо досягти переваги над противником в інформаційному компоненті, швидкості та якості управління військами. Сунь-цзи підкреслював важливість самоконтролю війська, глибокого аналізу ситуації і контролю можливостей свого та ворожого військ [2]. Підрозділами та засобами ОВТ ЗСУ керують командири, які використовують різноманітні інформаційно-технологічні системи. Відомо, що сучасні військові інформаційні системи використовують автоматизовані системи управління, інтелектуальні системи та різноманітні бази даних. Все більшу частку рішень в інформаційних системах надають системи штучного інтелекту. Системи штучного інтелекту (далі – СШІ) подовжують свій якісний та прикладний розвиток [3]. СШІ застосовуються в надскладних інформаційних системах, сучасних БпЛА, роботизованих морських системах, літаках, засобах РВіА для ефективного аналізу бойової обстановки та швидкого прийняття рішень тощо.

Відомо, що сучасні підходи побудови СШІ базуються на принципах роботи головного мозку людини (далі – ГМЛ) [5]. Автори вважають, що подальше вивчення загадок роботи ГМЛ надають науковцям та інженерам шляхи для розробки нових ефективних інформаційних систем, необхідних для успішного ведення сучасних мережецентричних війн [4]. Теоретики та практики вважають, що мозок людини на сучасному етапі переважає можливості навіть квантового комп’ютера.

Автори вирішили здійснити дослідження телекомунікаційних властивостей нейронів та нейронних ансамблів на основі припущень, які розглядають можливості збереження нейронами слідів інформації, придбаних у різні періоди часу Δt_n, та їх пов’язаності з нейронами інших почуттів людини або іншими функціональними угрупуваннями нейронів, навчених у цей же період часу Δt_n.

Аналіз публікацій за темою дослідження. Класична робота [6] щодо структури та функціоналу ГМЛ має один недолік – це її вік, бо дослідження викладені ще до масованого застосування комп’ютерних технологій. Тому в ній відсутній шар надсучасних досліджень. Але робота [6] може стати базовою для науковця, який планує дослідити принципи обробки інформації в ГМЛ. Автори вважають, що роботу можливо розглядати як початок для нових досліджень загадок у роботі ГМЛ.

Сучасна робота [7] щодо виявлення прихильності нейронних субстратів для розпізнавання обличчя розкриває можливості, механізми й алгоритми обробки візуальної інформації та підказує шляхи створення математичних і телекомунікаційних моделей ГМЛ. Недоліком роботи є те, що в ній не розкритті можливості збереження інформації в ГМЛ на нейронному рівні на кожному окремому відрізку часу.

Робота [8] дуже важлива тому, що вона аналізує спостереження за зоровим сприйняттям після роз’єднання півкуль головного мозку у людини та відповідає на сучасні питання науковців. Підказує науковцям шляхи опису функціоналу ГМЛ, який поступово досліджується та модулюється, а в подальшому реалізується в прикладних системах. Ця робота також є початком для практичного моделювання роботи ГМЛ.

У роботі [9] розглянуто повний курс нейронних мереж. Саме завдяки цьому курсу та новим ідеям, взятим з нових досліджень роботи нейрона та нейромережі, з’являється можливість проєктувати нові сучасні штучні мережі, саме чим і планують зайнятися автори у своїх дослідженнях.

У роботах [10–19] розглядаються останні дослідження роботи ГМЛ та проєктування схем і моделей штучних мереж.

Мета статті. Науковим завданням статті є спроба опису та дослідження додаткових можливостей нейрона ГМЛ та перенесення додаткових можливостей до опису штучного нейрона, в якому використовуються припущення щодо збереження шарами нейрона l_n слідів інформації, придбаної під час його життя Δt_n. Дослідження їхньої взаємопов'язаності з іншими групами нейронів відповідно до інших видів почуттів або функціональними ансамблями, навченими у той самий відрізок часу Δt_n.

Основний матеріал. Еволюція надала ГМЛ можливості, які відсутні у сучасних обчислювальних системах, створених відповідно до архітектури фон Наймана, до яких відносяться:

розподілення інформації і паралельні обчислення;

можливість навчання й узагальнення;

адаптивність;

толерантність до помилок.

Новітні досягнення в області нейрофізіології дають початкове розуміння механізмів природного мислення, де збереження інформації відбувається у виді складних образів та моделей. Новий процес обробки даних не використовує традиційне програмування, забезпечує створення паралельних мереж і їхнє навчання [5].

Перш за все автори роблять припущення, що новий живий нейрон на нижчому рівні послідовно запам'ятовує різноманітну базову інформацію i_n, тому що має декілька незалежних шарів пам'яті, які він використовує у різний період часу Δt_n.

Надалі нейрон може генерувати інформацію i_n, яка зафіксована у кожний період свого життя Δt_n, де n – деякий шар ядра нейрона відповідно до збудження від спеціалізованої групи нейронів, які контролюють сканування всього часу Δt та проміжків часу Δt_n.

Розглянемо будівлю біологічного нейрона. На рисунку 1 зображено базовий елемент нервової системи – нервову клітку, яку називають нейроном [5].

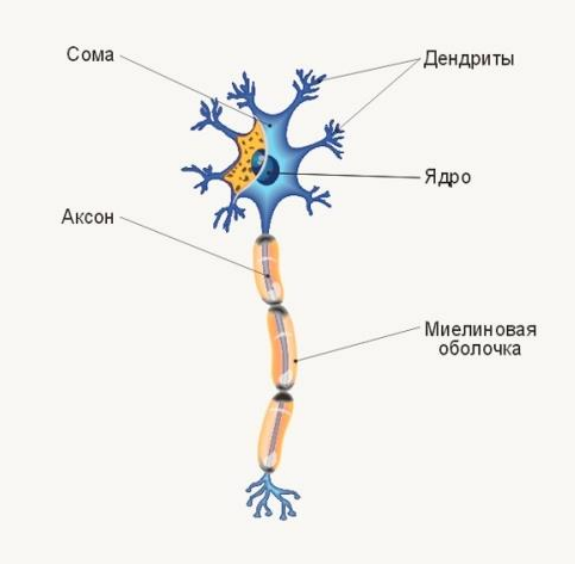

Рис. 1. Зображення нервової клітки – нейрона

У нейроні можна виділити тіло клітки, яке називають *сомою,* а також вихідні з нього два види відростків:

дендрити – вхід у нейрон, через який надходить інформація;

аксон – вихід нейрона, який передає інформацію.

На рисунку 2 зображена загальноприйнята у світі модель нейрона, в рамках якої автори починають дослідження.

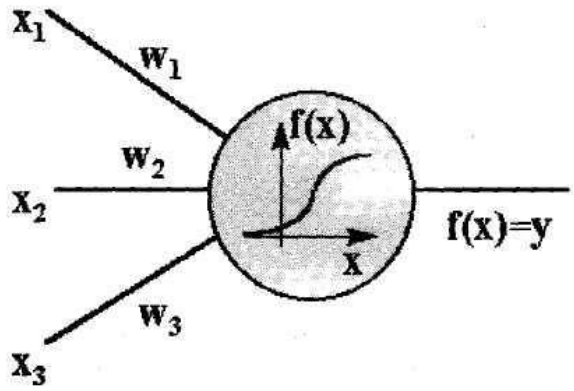

Рис. 2. Спрощена модель нейрона

На рисунку 2 зображена спрощена модель нейрона з трьома входами (дендритами), причому синапси цих дендритів мають ваги w_1, w_2, w_3. До синапсів надходять імпульси сили x_1, x_2, x_3 відповідно, тоді після проходження синапсів і дендритів до нейрона надходять імпульси $w_1 x_1$, $w_2 x_2$, $w_3 x_3$. Нейрон перетворює отриманий сумарний імпульс згідно з виразом (1):

$$x = w_1 x_1 + w_2 x_2 + w_3 x_3. \quad (1)$$

Кожний нейрон функціонує відповідно до деякої передатної функції $f(x)$. Сила вихідного імпульсу відповідає виразу (2):

$$y = f(x) = f(w_1 x_2 + w_2 x_2 + w_3 x_3). \quad (2)$$

Отже вважається, що нейрон цілком описується своїми вагами w_k і передатною функцією $f(x)$. Одержавши набір чисел (вектор) w_k як входи, нейрон видає деяке число y на виході.

На рисунку 3 надана узагальнена модель нейрона, зв'язана з першими спробами формалізувати опис функціонування нервової клітки [4].

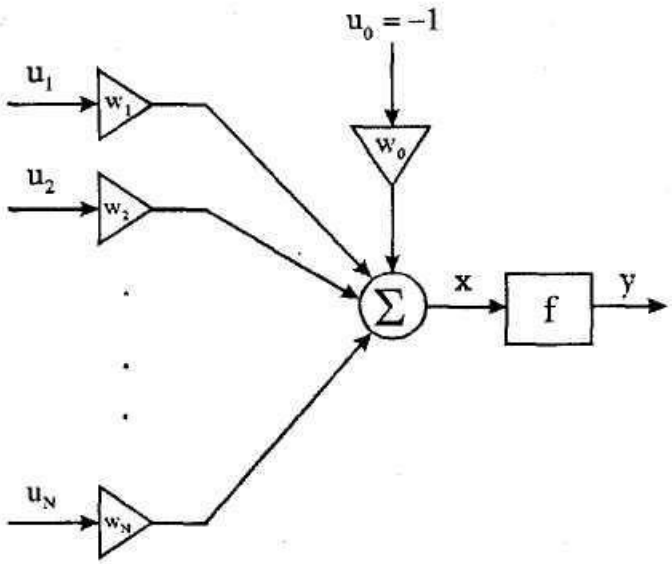

Рис. 4. Узагальнена модель нейрона

Використовуються наступні позначення:
u_1, ..., u_N – вхідні сигнали нейрона, які приходять від інших нейронів;
w_1, ..., w_N – синаптичні ваги;
y – вихідний сигнал нейрона;
v – граничне значення.
Формула, що описує функціонування нейрона, має вигляд (3):

$$\begin{cases} 1 \quad \text{при} \quad \sum w_i x_i \geqslant v, \\ 0 \quad \text{при} \quad \sum w_i x_i \leqslant v. \end{cases} \tag{3}$$

Модель може бути представлена виразами (4), (5):

$$y = f(\sum_{i=0}^{N} w_i u_i), \tag{4}$$

де

$$f(x) = \begin{cases} 1 \text{ при } x \geq 0, \\ 0 \text{ при } x < 0. \end{cases} \tag{5}$$

а також $w_0 = v$, $u_0 = 1$.

Формула (4) описує модель нейрона, представлену на рисунку 4. Ця модель була запропонована в 1943 р. Маккаллоком і Питтсом [5]. В якості функції f може прийматися не тільки одинична функція (5), але й інші граничні функції виду (6), (7):

$$f(x) = \begin{cases} 1 \text{ при } x \geq 0, \\ -1 \text{ при } x < 0. \end{cases} \tag{6}$$

або

$$f(x) = \begin{cases} 1 \text{ при } x \geq 0, \\ -1 \text{ при } x < -1, \\ x \text{ при } |x| \leqslant 1. \end{cases} \tag{7}$$

На початковій фазі моделювання біологічних нейронних мереж застосовувалися граничні функції (5)–(7). Нині найчастіше використовується сігмоїдальна функція, яка обумовлена виразом (8):

$$f(x) = \frac{1}{1+e^{-\beta x}} > 0. \tag{8}$$

Відзначимо, що при $\beta \to \infty$ характеристика (8) прагне до граничної уніполярної функції (5). Як альтернатива застосовується функція гіперболічного тангенса згідно з виразом (9):

$$f(x) = th\left(\frac{\alpha x}{2}\right) = \frac{1-e^{-\beta x}}{1+e^{-\beta x}} > 0. \tag{9}$$

У цьому випадку характеристика (9) прагне до граничної біполярної функції (6) при $\alpha \to \infty$. Приклади функції f у моделі (4) показані на рисунку 4.

На рисунку 5 зображені відомі приклади передаточної функції f.

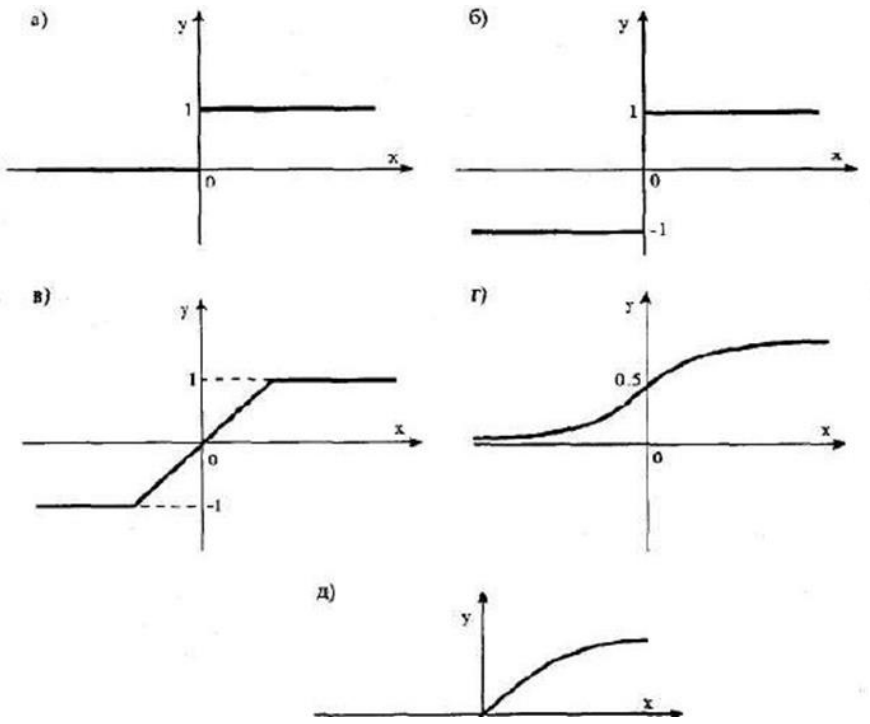

Рис. 5. Приклади функції *f* (*x*)

У існуючих зараз програмних розробках штучні нейрони називають «елементами обробки» і вони мають більше можливостей, ніж простий штучний нейрон, описаний вище. На рисунку 6 зображена детальна схема спрощеного штучного нейрона.

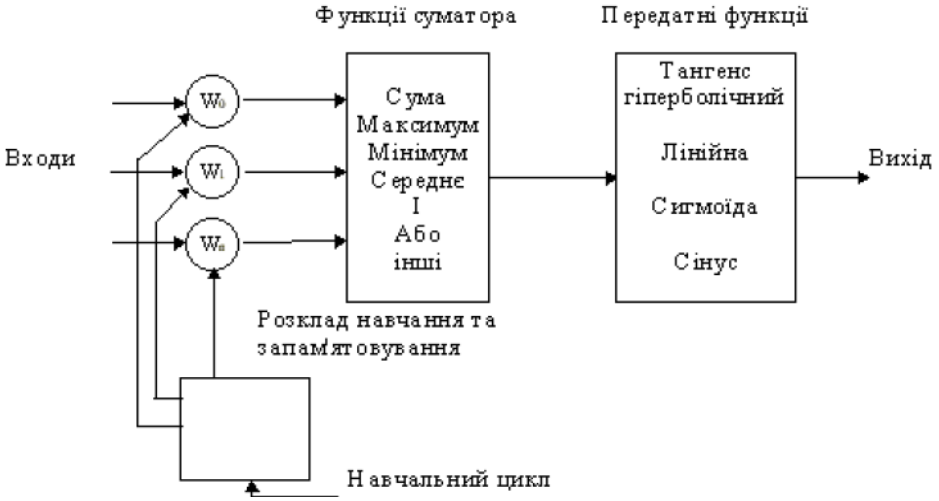

Рис. 6. Схема спрощеного штучного нейрона

Доопрацьовані входи передаються на функцію підсумовування добутків. Можна вибрати різні операції, такі як середнє арифметичне, найбільше, найменше, OR, AND і ті, що виробляють різні значення. Більшість комерційних програм дозволяють створювати власні функції суматора за допомогою підпрограм, закодованих мовою високого рівня. Іноді функція підсумовування модифікується додаванням функції активації, що дозволяє функції підсумовування діяти в часі. У кожнім з цих випадків вихід функції підсумовування проходить через передатну функцію на вихід (0 або 1, -1 або 1, чи будь-яке інше число) за допомогою визначеного алгоритму. В існуючих нейромережах як передатні функції можуть бути

використані сігмоїда, синус, гіперболічний тангенс та ін. Приклад того, як працює сігмоїдна передатна функція, показано на рисунку 7.

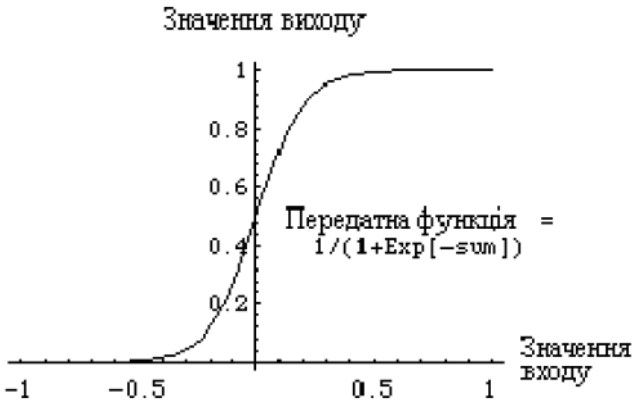

Рис. 7. Сігмоїдна передатна функція

Усі штучні нейромережі конструюються з базового блоку – штучного нейрона. Існуючі розмаїтості і відмінності є підставою для мистецтва талановитих розробників при реалізації ефективних нейромереж [9].

Автори цієї статті роблять наступні припущення щодо додаткових властивостей одного живого нейрона, а відповідно і моделюють штучний:

ядро живого нейрона ГМЛ має багатошарову l – *leare* структуру $l_1 \ldots l_N$, де N – загальна кількість внутрішніх шарів ядра;

шари нейрона l_n під час загального життя нейрона $\Delta t = (t_0 – t_N)$ здатні послідовно у часі фіксувати різні відбитки інформації – i_n в діапазоні значень (-1…1);

шари нейрона l_n здатні віддавати відбитки інформації – i_n відповідного періоду фіксації $\Delta t_n = (t_{n-1} – t_n)$;

пусковий сигнал $d(\Delta t_n)$ для видачі відбитка інформації – $i(\Delta t_n)$ надає дендрит-канал k-d_j, поєднаний з керуючою групою нейронів, яка призначена для сканування шарів нейронів, навчених у різних часових проміжках Δt_n;

схожий пусковий сигнал $d(\Delta t_n, s_p)$ надає інший дендрит-канал k-d_j-s_p, поєднаний з іншою групою сенсорних нейронів – s_p, пов’язаних із різними видами почуттів людини або іншими функціональними ансамблями, навченими в тому самому проміжку часу Δt_n.

На рисунку 8 можна побачити підстави для формування викладених вище припущень.

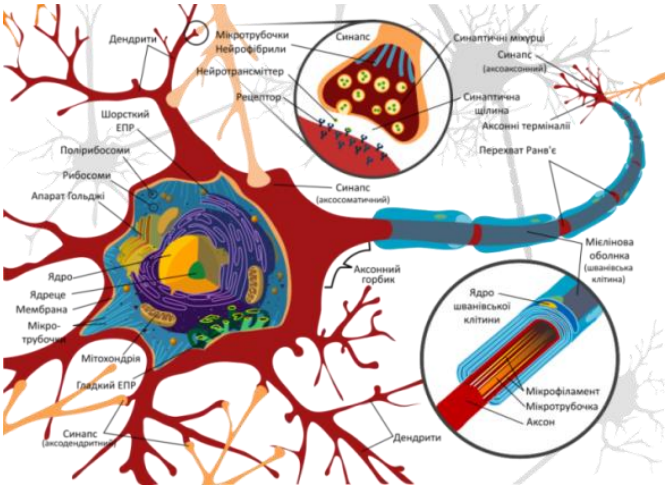

Рис. 8. Приклад зображення живого нейрона, шари ядра якого вказують на його поширені можливості

На рисунку 9 наведено спрощену схему нейрона, ядро якого здатне зберігати велику кількість слідів інформації $i(t_n)$. При цьому нейрон здатен одночасно бути поєднаним та задіяним у різних функціональних нейронних ансамблях, які виконують різні функції. Саме такі властивості одного штучного нейрона (далі – ШН) нададуть складеній з ШН штучній мережі (далі – ШМ) такі вади, які наблизять її здатності до можливостей людини.

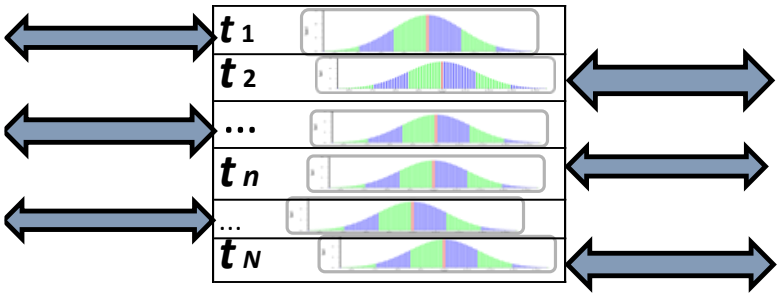

Рис. 9. Модель нейрона, здатного зберігати вектор інформаційних слідів, зафіксованих у різні періоди часу життя нейрона

Додатково рисунок 9 пояснює, як один нейрон бере участь у різноманітних функціональних ансамблях ГМЛ. Інформація в кожному шарі постійно регенерується з частотою приблизно 10 Гц. При припиненні процесу регенерації інформація знищується і відновленню не підлягає [12].

Автори вважають, що відомий опис нейрона з функцією (2) слід трактувати ширше згідно з виразом (10):

$$y = f(\sum_{i=0}^{N} w_i u_i), \tag{10}$$

Розглянемо **перше** припущення авторів, якщо вхід x ~ *відповідає відрізку* Δt_n, тоді збереження слідів інформації – i_n відповідає періоду часу навчання $\Delta t_n = (t_{n-1} - t_n)$ у шарі нейрона – l_n, тоді формула, що описує функціонування нейрона, має вигляд (11):

$$\begin{cases} i_1 \ \text{при} \ x_1 \subset \Delta t_1 \\ i_2 \ \text{при} \ x_2 \subset \Delta t_2 \\ \quad\quad ... \\ i_n \ \text{при} \ x_n \subset \Delta t_n \\ \quad\quad ... \\ i_N \ \text{при} \ x_N \subset \Delta t_N \end{cases}, \tag{11}$$

де $i_n \in (-1, \ldots, 1)$;

$n = 0, \ldots, N$;

N – максимальна кількість шарів нейрона.

На рисунку 10 зображено поширену модель нейрона відповідно **до першого** припущення авторів.

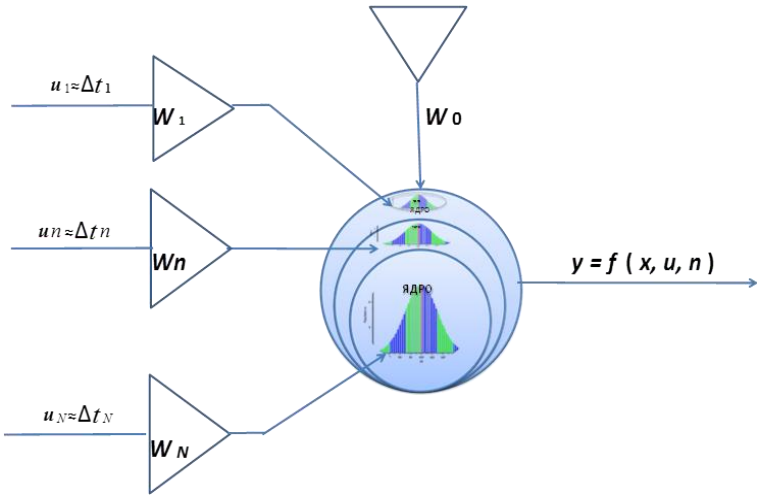

Рис. 10. Модель нейрона згідно з першим припущенням авторів

Друге припущення авторів – $x \sim d(\Delta t_n, s_p)$ – стосується поєднання нейрона дендрит-каналом з групою сенсорних нейронів – s_p, пов'язаних з іншим почуттям людини або функціональним ансамблем, навчених на одному проміжку часу Δt_n. Тоді формула, що описує функціонування нейрона, має вигляд (12):

$$\begin{cases} i_1 \ \text{при} \ x_1 \subset \Delta t_1, s_p \\ i_2 \ \text{при} \ x_2 \subset \Delta t_2, s_p \\ \quad \dots \\ i_n \ \text{при} \ x_n \subset \Delta t_n, s_p \\ \quad \dots \\ i_N \ \text{при} \ x_N \subset \Delta t_N, s_p \end{cases}, \tag{12}$$

де s_p поєднана з нейроном групи нейронів одного з почуттів людини або функціонального ансамблю;

p – група одного з видів почуттів людини (зір, слух, смак, нюх, дотик, біль, температура, вестігулярність та ін.) або функціонального ансамблю;

P – загальна кількість видів почуттів людини, утворених на одному проміжку часу Δt_n або функціонального ансамблю.

Загальну модель такого нейрона автори представляють наступними виразами (13), (14):

$$y = f\left(\sum_{i=0}^{N} w_i u_i, \Delta t_N, s_p\right), \tag{13}$$

де

$$y = f(s_p, \Delta t_n) = \begin{cases} f(x_1) \ \text{при} \ x_1 \subset \Delta t_1 \\ f(x_2) \ \text{при} \ x_2 \subset \Delta t_2 \\ \quad \dots \\ f(x_n) \ \text{при} \ x_n \subset \Delta t_n \\ \quad \dots \\ f(x_N) \ \text{при} \ x_N \subset \Delta t_{N2} \end{cases}. \tag{14}$$

На рисунку 11 автори зображають передатну функцію запропонованого нейрона.

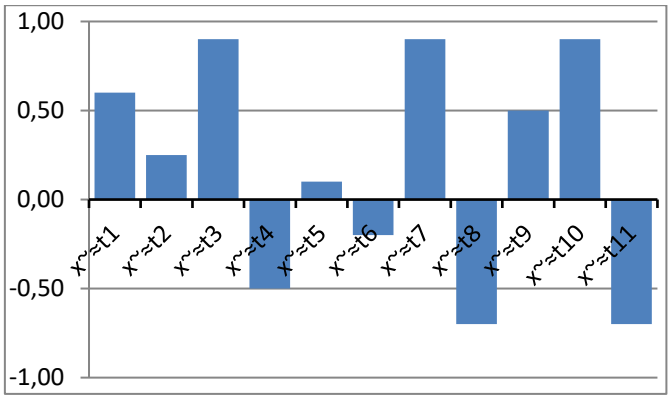

Рис. 11. Передатна функція поширеного нейрона, навченого за загальне Δt_n

На рисунку 12 автори зображають модель нейрона з урахуванням відрізку часу навчання (Δt_n) та пов'язаності нейрона з групою нейронів одного з видів почуттів або функціональним ансамблем.

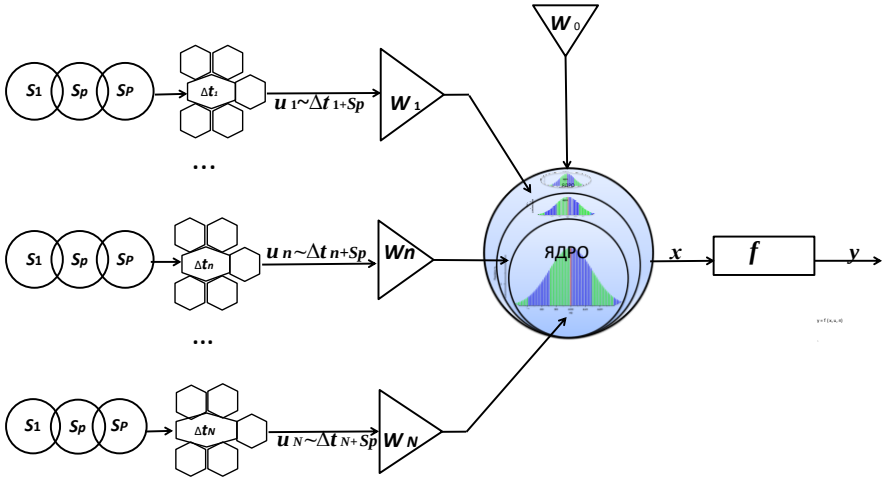

Рис. 12. Схема моделі нейрона з урахуванням відрізку часу навчання та групи сенсорів почуттів або функціональним ансамблем, навчених в Δt_n

Авторами запропонована спрощена таблиця, яка пояснює зовнішні зв'язки нейрона з поширеними можливостями (табл. 1).

Таблиця 1

Взаємозв'язки нейрона з поширеними можливостями

Група сканування часових шарів нейрона		s_1	s_2	…	s_p	…	s_P
	Δt_1	$i(\Delta t_1,s_1)$	$i(\Delta t_1,s_2)$	…	$i(\Delta t_1,s_p)$	…	$i(\Delta t_1,s_P)$
	Δt_2	$i(\Delta t_2,s_1)$	$i(\Delta t_2,s_2)$	…	$i(\Delta t_2,s_p)$	…	$i(\Delta t_2,s_P)$
	…	…	…	…	…	…	…
	Δt_n	$i(\Delta t_n,s_1)$	$i(\Delta t_n,s_2)$	…	$i(\Delta t_n,s_p)$	…	$i(\Delta t_n,s_P)$
	…	…	…	…	…	…	…
	Δt_N	$i(\Delta t_N,s_1)$	$i(\Delta t_N,s_2)$	…	$i(\Delta t_N,s_p)$	…	$i(\Delta t_N,s_P)$

Спрощений алгоритм навчання та використання нейрона з поширеними можливостями виглядає так:

1. Деякий шар – l нейрона $\eta(\Delta t_n, p)$ – в групі p було навчено у відрізок часу Δt_n.

2. У цей же період Δtn було навчено взаємопов'язаний нейрон $\eta(\Delta t_n, p \pm 1)$ з деякої іншої групи $p \pm 1$.

3. Пошук інформації здійснюється шляхом поетапного перебору всіх шарів – l нейрона за рахунок послідовного збудження нейронного вектору $\eta(\Delta t_n)$.

4. Надалі збудження обраного нейрона $\eta(\Delta t_n, p)$ призведе до збудження взаємопов'язаного з ним нейрона $\eta(\Delta t_n, p \pm 1)$.

5. Надалі механізми навчання або розпізнавання здійснюється паралельно в різних функціональних ансамблях. Це призведе до взаємного підтвердження результатів та підвищення адекватності результатів. Наприклад, механізми градієнтного спуску стосовно навчання згідно з деяким завданням буде здійснюватися одночасно в різних нейронних ансамблях.

Авторами пропонується спрощений рисунок, який пояснює зв'язки нейрона з поширеними можливостями з нейронами інших груп почуттів або функціональних ансамблів (рис. 13).

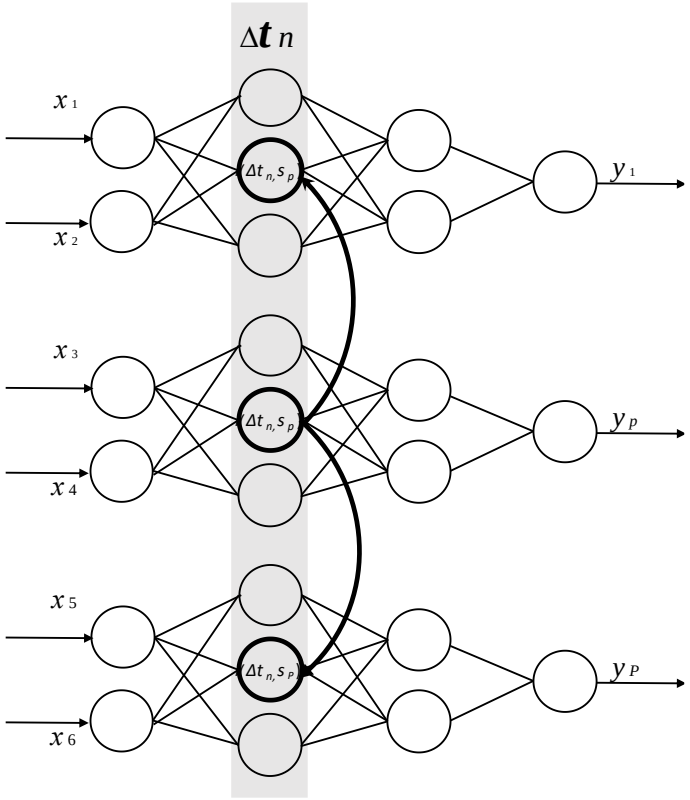

Рис. 13. Схема зв'язків нейрона з нейронами інших груп почуттів або функціональних ансамблів

Автори вважають наступне:

кожний нейрон навчається у своєму функціональному ансамблі одночасно з іншими нейронами з груп інших функціональних призначень;

нейрон пов'язаний дендрит-синапс-аксоновою схемою з нейроном іншого ансамблю, що навчається у той самий період часу за тим самим завданням;

різні нейронні функціональні групи одночасно вирішують одну базову задачу. Зазвичай базовою є задача розпізнавання, передбачення і тому подібне. У більшості випадків її можна трактувати як задачу про заповнення пропусків в даних.

На рисунку 14 показано, що в ГМЛ різними нейронними ансамблями деяка базова задача одночасно вирішується багатьма пов'язаними ансамблями нейронів.

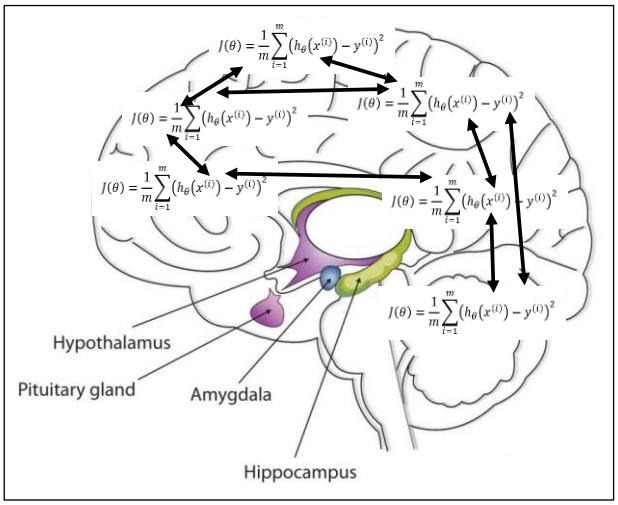

Рис. 14. Одночасне рішення базової задачі багатьма функціональними ансамблями в ГМЛ

Автори вважають, що подібний зв'язок замало вивчено та враховано у штучних нейромережах. Адже саме такі зв'язки дають людині перевагу над ШМ!

На рисунку 15 зображено цікаве порівняння вигляду квантових комп'ютерів з біологічними нейронними ансамблями, які нагадують деякий ансамбль люстр.

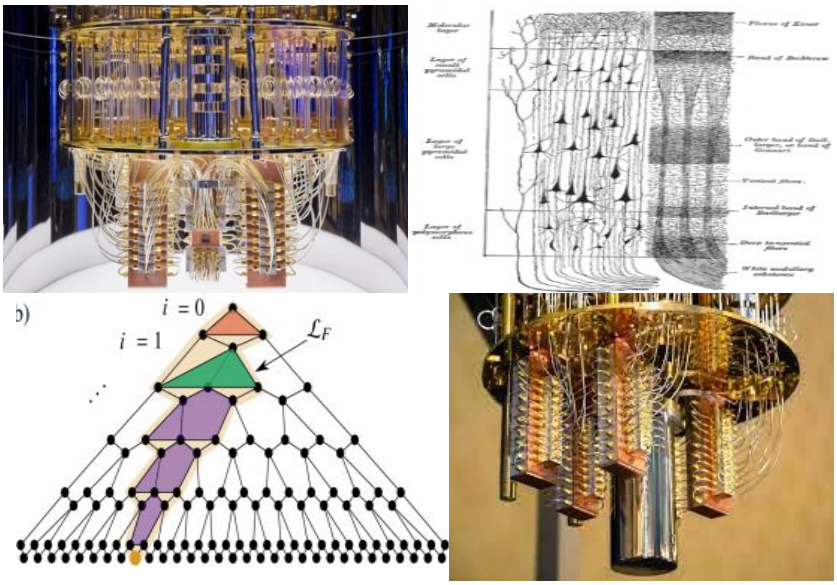

Рис. 15. Порівняння вигляду квантових комп'ютерів з біологічними нейронними ансамблями

Висновки. Отже, в статті розглянуті наступні припущення авторів:

про можливість нейрона, завдяки його багатошаровості, зберігати сліди пам'яті, зафіксовані у різний період функціонування нейрона;

про те, що кожний нейрон є часткою ансамблю, який відповідає за одну функцію одного з видів почуттів, а саме зору, слуху, смаку, нюху, дотику, болю та температури;

всі нейрони взаємопов'язані з нейронами іншого функціонального ансамблю. Така спеціалізація відсутня у автоматів та ШМ, тому в них немає природньої мотивації.

Подальші шляхи досліджень передбачають розгортання досліджень щодо шляхів утворення часових врім'янок слів, думок, мислення, наукового мислення та їхніх математичної і телекомунікаційної моделей. Подальші дослідження функціонального

призначення ансамблів нейронів та створення їхніх математичної, програмної та телекомунікаційної моделей.

Також подальші шляхи досліджень авторів можуть торкатися таких напрямків:

Опис алгоритму роботи мережі, створеної зі штучних пов'язаних нейронів $\eta(\Delta t_n)$;

Опис роботи мережі, складеної з шарів нейронів, навчених за один відрізок часу Δt_n;

опис роботи мережі, складеної з шарів нейронів різних видів почуттів або функціональних ансамблів $\eta(\Delta t_n, s_p)$;

опис роботи окремої мережі, яка фіксує схеми зв'язків запропонованих вище мереж η-η-η-$(\Delta t_n, s_p)$.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Б. Лиддел Гарт. Вторая мировая война / сост. С. Переслегин, Р. Исмаилов. М.: ООО «Фирма «Издательство АСТ»; СПб.: Terra Fantastika, 1999. 944 с.: ил. (Военно-историческая библиотека). ISBN 5-237-03175-7. ISBN 5-7921-0260-0.

2. Сунь-цзи. Мистецтво війни / пер. з англ. Ганни Литвиненко. Харків: Книжковий Клуб «Клуб Сімейного Дозвілля», 2016. 127 с.: кольор. іл. ISBN 978-617-12-1514-6 (укр.).

3. Системи штучного інтелекту: навч. посіб. 2-ге вид., виправ. та доп. / Ю. В. Нікольський, В. В. Пасічник, Ю. М. Щербина; за наук. ред. В. В. Пасічника. М-во освіти і науки, молоді та спорту України. Львів: Магнолія – 2006, 2013. 279 с.: іл. (Серія «Комп'ютинг»). Бібліогр.: С. 275–278 (58 назв). ISBN 978-617-57-40-11-4.

4. Нас ждут сетецентрические войны // Україна кримінальна. URL: https://cripo.com.ua/processes/?p=135749/.

5. Кононюк А. Ю. Нейронні мережі і генетичні алгоритми. Київ: Корнійчук, 2008. 446 с.

6. Блум Ф., Лейзерсон А., Хофстедтер Л. Мозок, разум і поведінка. Редакція біологічної літератури / Переклад з англ. канд. біол. наук Є. З. Годіної // RoyalLib: електронна бібліотека. URL: https://royallib.com/book/blum_floyd/mozg_razum_i_povedenie.html (дата звернення: 19.10.2022).

7. Фарах М. Дж., Рабіновиц К., Куїнн Г. Е., Лю Г. Т. Рання прихильність нейронних субстратів для розпізнавання обличчя// Когнітивна нейропсихологія. 2000. № 17 (1–3). С. 117–123.

8. Газзаніга М. С., Боген Дж., Сперрі Р. В. Спостереження за зоровим сприйняттям після роз'єднання півкуль головного мозку у людини // Мозок. 1965. № 88 (2). С. 221–236.

9. Хайкин С. Нейронные сети: полный курс. 2-е изд., испр. Пер. с англ. М.: ООО «И. Д. Вильямс», 2006. 1104 с.

10. Де Кортен-Майєрс Г. М. Кора головного мозку людини: гендерні відмінності в будові та функції // Журнал невропатології та експериментальної неврології.1999. № 58. С. 217–226.

11. Нова модель сприйняття: наш мозок бачить дуже багатий світ // Конкурент: інформаційне агентство. URL: https://konkurent.ua/publication/54312/nova-model-spriynyattya-nash-mozok-bachit-duzhe-bagatiy-svit/ (дата звернення: 19.10.2022).

12. Best Ben. The Amygdala and the Emotions // Ben Best: website. URL: http://www.benbest.com/science/anatmind/anatmd9.html.

13. Фокс Дж. Л. Динамічний спосіб мозку підтримувати зв'язок // Наука. 1984. № 225 (4664). С. 820–821.

14. Фріч Г., Хітціг Е. Електрична збудливість головного мозку (Über die Electrische erregbarkeit des Grosshirns) // Епілепсія та поведінка. № 15 (2). С. 123–130. (Оригінальний твір опублікований 1870 р.).

15. Гібсон К. Р. Еволюція людського інтелекту: ролі розміру мозку та розумової побудови // Поведінка мозку та еволюція. 2002. № 59. С. 10–20.

16. Мартін А. Представлення предметних понять в мозку // Щорічний огляд психології. № 58. С. 25–45.

17. Шерман С. М., Гільлери Р. В. Дослідження таламуса і його ролі в корковій функції (2-ге вид.). Кембридж, Массачусетс: MIT Press, 2006.

18. Уайлд Д. Дж. Методы поиска экстремума. М.: Главная редакция физико-математической литературы издательства «Наука», 2017. 268 с.

19. Цікаві факти про людський мозок. Частина II // URL: https://lc-neuro.com.ua/blog/czikavi-fakti-pro-lyudskij-mozok-chastina-ii (дата звернення: 19.10.2022).

УДК 341:004

Лазута Р. Р. ORCID: 0000-0003-3254-9690 (ВІТІ ім. Героїв Крут)
Зінченко М. О. ORCID: 0000-0002-1428-8231 (ВІТІ ім. Героїв Крут)
Яковчук О. В. ORCID: 0000-0002-6312-5009 (ВІТІ ім. Героїв Крут)
Макарчук В. І. ORCID: 0000-0002-3997-4684 (ВІТІ ім. Героїв Крут)

АНАЛІЗ ПІДХОДІВ ПРОВІДНИХ КРАЇН СВІТУ ДО ВЕДЕННЯ КІБЕРВІЙН ТА КІБЕРОПЕРАЦІЙ

У статті розглянуто аналізи підходів провідних країн світу та країн-членів НАТО до ведення кібервійн та кібероперацій і застосування, впровадження й заміна цих підходів в нашій державі в цілому.

У війнах і збройних конфліктах минулого століття, у класичному їх розумінні, з «нематеріальних» технологій протиборства застосовувалися, як відомо, переважно лише методи інформаційно-психологічної боротьби як механізм впливу на свідомість людини, а також дезінформації населення і Збройних сил супротивника.

Саме такий стан справ, по-перше, обумовив нові завдання для Збройних сил і компетентних державних правоохоронних органів провідних країн світу, які мають спрямовуватися на забезпечення протидії або на повну нейтралізацію різного роду кіберзагроз; по-друге, підняв на беззаперечно вищий щабель вагу досліджень, спрямованих на розроблення методології кібервоєн та прогнозування довгострокових тенденцій їхнього розвитку, вироблення актуальних моделей проведення атакуючих дій у кіберпросторі, а також створення систем ефективної протидії останнім.

Тобто, як бачимо, тема кібервійни останнім часом доволі активно досліджується представниками більшості провідних країн світу. Увагу цьому питанню приділяють також і військові блоки. Так, у керівних документах НАТО та країн-членів НАТО кібервійна розглядається в одному ряду з протиракетною обороною та боротьбою з тероризмом.

Під кібероперацією, за аналогією з методами звичайної війни, розуміють сукупність узгоджених за часом, глибиною та завданнями відносно короткочасних кібератак, спрямованих на один або декілька об'єктів впливу протиборчої сторони з наміром одержання незаконного доступу до їх інформаційних ресурсів, порушення роботи їхніх інформаційних систем або взагалі повного виведення обраних об'єктів з функціонування.

Тобто, якщо взяти до уваги головні характеристики майбутніх кібервоєн, а саме: можливість здійснення нападу ким-небудь; географічну досяжність; невідворотність; потенціал і легкість поширення, а також вплив на «електронно готові» цілі, – можна припустити, що їхній початок може стати революцією у військовій справі, а їхні результати взагалі можуть виявитися непередбачуваними.

Отже, пропонується змінити прийняті в нашій державі підходи до визначень та термінологічних взаємозв'язків між кіберопераціями та кібердіями, розробити та впровадити відповідні документи, закупити новітні засоби зв'язку для розвитку новітніх ІТ-технологій країни.

Ключові слова: *НАТО, кібервійна, кібероперація, кіберзагроза.*

R. Lazuta, M. Zinchenko, O. Yakovchuk, V. Makarchuk Analysis of approaches of leading countries of the world to conducting cyber wars and cyberoperations.

The article examines analysis of the approaches of the world's leading countries and NATO member states to the conduct of cyber wars and cyber operations and the application, implementation and replacement of these approaches in our country as a whole.

In the wars and armed conflicts of the last century, in their classical sense, with "intangible" technologies of confrontation were used, as is known, mainly only methods of information and psychological struggle as a mechanism of influence on human consciousness and misinformation of the population and armed forces of the opponent.

It is this state of affairs that has, firstly, set new challenges for the Armed Forces and the competent state law enforcement agencies of the world's leading countries, which must be aimed at ensuring the counteraction or complete neutralization of various types of cyber threats; secondly, it raised to an unequivocally higher level the weight of research aimed at developing cyber warfare methodologies and forecasting long-term trends in their development, developing current models of attacking actions in cyberspace, and creating systems to effectively counter the latter.

That is, as we see, the topic of cyber warfare has recently been quite actively studied by representatives of most leading countries in the world. Military blocs are also paying attention to this issue. Thus, in the guiding documents of NATO and NATO member countries, cyber warfare is considered on a par with missile defense and the fight against terrorism.

Under cyber operation, by analogy with the methods of conventional warfare, is a set of agreed on time, depth and objectives for short-term cyberattacks aimed at one or more objects of influence of the opposing side with the intention

of gaining illegal access to their information resources, disruption of their information systems or complete withdrawal of selected objects from operation.

That is, given the main characteristics of future cyber wars, namely: the possibility of an attack by someone; geographical reach; inevitability; the potential and ease of dissemination, as well as the impact on "electronically prepared" targets, suggest that their onset may be a military revolution, and their results may be unpredictable.

Thus, it is proposed to change the approaches adopted in our country to the definition and terminological relationships between cyber operations and cyber actions, to develop and implement relevant documents and purchase the latest communications for the development of the latest IT technologies in the country.

Keywords: *NATO, cyber war, cyber operation, cyber threat.*

Постановка завдання. Більшість аспектів військових операцій Збройних сил України частково покладаються на використання кіберпростору, який в нашому сьогоденні є водночас як невід'ємною сферою інформаційного середовища, так і тією субстанцією, яка, з аналогію будь-якого визначення «системи», є одночасно й елементом цієї системи, і тією прихованою «силою» («відношенням»), що зумовлює взаємодію елементів інформаційного середовища між собою.

Якщо розглянути підходи до визначення «кіберпростір», наведені в керівних документах більшості країн-членів НАТО, зокрема США, кіберпростір являє собою (в буквальному перекладі різних організацій) – «Глобальний домен в інформаційному середовищі, що складається із взаємозалежних мереж інфраструктур інформаційних технологій та даних резидентів, включаючи Інтернет, телекомунікаційні мережі, комп'ютерні системи та вбудовані процесори і контролери» (документи JP 3-12 та FM 3-12).

Із огляду на викладене, стає зрозумілим багаточисельне обговорення тем, пов'язаних з кіберпростором та так званими «кібердіями» (визначення яких відсутнє на загальнодержавному рівні і навіть якщо з'явиться, то буде періодично змінюватись). Але все ж таки, у зв'язку із їх «віртуальною» наявністю, ця робота спрямована саме на їх розгляд та удосконалення в інтересах нашої держави.

Розвиток інформаційного суспільства дозволяє використовувати кіберпростір для вирішення політичних, соціокультурних та воєнних завдань (прості приклади: Крим, Донбас), можливості прихованого впливу на підсвідомість людей і масштабного маніпулювання суспільною думкою завдяки використанню інформаційних технологій та засобів масових комунікацій, не кажучи вже при цьому про ще ряд аспектів, пов'язаних, наприклад, із дистанційним ураженням як військових, так і цивільних об'єктів, особливо в мирний час. Це постійно призводить до появи нових форм і методів кібердій, завдяки яким провідні держави намагаються досягти своїх зовнішньополітичних цілей і владнати міждержавні розбіжності.

У сучасному світі зазначене відбувається через використання (звичайно приховано) кібердій у кіберпросторі, форми і способи яких постійно удосконалюють спеціальні (визначені) підрозділи провідних країн світу.

У цих умовах підрозділи кібербезпеки Збройних сил України повинні постійно вживати заходів для удосконалення форм та способів кібердій в рамках готовності до кібероборони держави.

Аналіз останніх досліджень і публікацій. Розвиток подій на міжнародній арені наприкінці XX – на початку XXI століття свідчить, що, попри потужні зусилля світової спільноти з урегулювання міждержавних суперечностей мирним шляхом, кількість і гострота збройних конфліктів сучасності практично не зменшуються. Більше того, нині вони охоплюють не тільки традиційні сфери збройної боротьби (землю, море, повітря), а й поступово просуваються в новітні сфери, наприклад, у віртуальний комп'ютерний світ, який практично є основою життя сучасної людини.

У війнах і збройних конфліктах минулого століття, у класичному їх розумінні, з «нематеріальних» технологій протиборства застосовувалися, як відомо [1], переважно лише

методи інформаційно-психологічної боротьби як механізм впливу на свідомість людини, а також дезінформації населення і Збройних сил супротивника. При цьому обладнання зв'язку та засоби масової інформації розглядалися тоді переважно як середовище для перенесення думки, потрібної передусім атакуючій стороні.

Із появою феномена глобальних комп'ютерних мереж з'явився , так званий, новий театр воєнних дій – кіберпростір, де поступово почали:

використовуватися принципово нові, специфічні засоби й методи ураження – інформаційна і кіберзброя, та формуватися тактика і стратегія їх застосування;

розгортатися угруповання сил і спеціальних програмно-апаратних засобів для проведення активних операцій (дій);

розвиватися засоби й методи захисту тощо.

На думку колишнього заступника міністра оборони США Елвіна Бернштейна, кібервійну в нинішніх умовах можна розглядати як складову загального театру воєнних дій, «як технологічний крок уперед у розвитку сучасних засобів і методів ведення війни та завдання ударів по системах командування і контролю противника». При цьому «комп'ютеризація даної сфери» та поява «нових засобів зв'язку й комунікацій», у розумінні екзаміністра, неминуче зробить саме такі засоби «об'єктами військового нападу». Американський журнал «The Economist», крім того, описує кібервійну як «п'яту область війни, – після землі, моря, повітря й космосу» [3]. Інший американський експерт з безпеки Річард А. Кларк у своїй книзі «Cyber War» (перша редакція якої вийшла у травні 2010 р.) визначає кібервійну як «дії однієї національної держави з проникнення в комп'ютерні мережі іншої національної держави для досягнення цілей щодо завдання збитку або руйнування» [4]. Державний секретар США Гіларі Клінтон, представляючи у травні 2011 р. «Національну стратегію в кіберпросторі», зробила заяву про можливість відповіді держави на будь-які прояви кіберагресії збройними засобами, якщо інші способи виявилися неефективними. Український вчений О. О. Мережко вважає кібервійну сукупністю заходів з «використанням Інтернету і пов'язаних з ним технологічних та інформаційних засобів однією державою з метою заподіяння шкоди військовій, технологічній, економічній, політичній та інформаційній безпеці, а також суверенітету іншої держави» [5].

Метою статті є аналіз підходів провідних країн світу до ведення кібервійн та кібероперацій застосування, впровадження і заміна цих підходів в нашій державі в цілому.

Виклад основного матеріалу. Досвід війн і воєнних конфліктів підтверджує, що успіх ведення бойових дій, поряд з іншими факторами, буде у тієї сторони, яка більш оперативно приймає рішення та своєчасно організовує їхнє виконання. Більш-менш чітке тлумачення поняття кіберпростір вперше було надано в директиві президента США «Національна стратегія гарантування безпеки кіберпростору США» (NSPD 54, 2004), кіберпростір визначений як взаємозалежна мережа комп'ютерних технологій, на яку спираються ведення бізнесу, дії уряду, керівництво національною обороною тощо [2].

Саме такий стан справ, по-перше, обумовив нові завдання для Збройних сил і компетентних державних правоохоронних органів провідних країн світу, які мають спрямовуватися на забезпечення протидії або на повну нейтралізацію різного роду кіберзагроз; по-друге, підняв на беззаперечно вищий щабель вагу досліджень, спрямованих на розроблення методології кібервоєн та прогнозування довгострокових тенденцій їхнього розвитку, вироблення актуальних моделей проведення атакуючих дій у кіберпросторі, а також створення систем ефективної протидії останнім.

Тобто, як бачимо, тема кібервійни останнім часом доволі активно досліджується представниками більшості провідних країн світу. Увагу цьому питанню приділяють також і військові блоки. Так, у керівних документах НАТО кібервійна розглядається в одному ряду з протиракетною обороною та боротьбою з тероризмом.

НАТО сьогодні має три лінії кібероборони (а саме: службу NATO Computer Incidents Response Capabilities Centre, Гаазький дослідницький центр перевірки діючих систем і вироблення новітніх стандартів захисту та Програму розробки захищених систем зв'язку), з метою підвищення ефективності ведення воєнних дій саме в кіберпросторі та додатково розробляє:

спеціальну структуру для захисту країн-членів Альянсу від кібератак, яка займатиметься збиранням розвідувальних даних і координуватиме дії членів НАТО в боротьбі з кіберзлочинністю;

концепцією майбутніх кібервійн, в основу якої покладено насамперед військово-технічну концепцію C4I (Command, Control, Computer, Communications and Intelligence) та C4IFTW (Command, Control, Computer, Communications and Intelligence for the Warrior), а також доктрину кіберманевру, що передбачає поділ усього театру воєнних дій на дві складові – традиційний та кіберпростори (ідея запропонована ще у 1996 р. експертом Пентагону Р. Банкером).

Так, у світі вже передбачається проведення як оборонних (захист власних ІТ-систем від деструктивного впливу), так і наступальних дій (встановлення контролю над ІТ-системами супротивника або взагалі їх знищення). При цьому основною формою таких дій, з урахуванням пропозицій [6], на тактичному рівні слід вважати кібератаки, на стратегічному та спеціальному рівнях – кібероперації, основні методи яких наведено в таблиці 1.

Таблиця 1

Основні методики кібератак, тактичних, стратегічних та спеціальних кібероперацій

Рівень операцій	***Основні методики проведення***
Тактичний	Ускладнення чи вибіркове зупинення діяльності телекомпаній, операторів стільникового зв'язку, провайдерів Інтернет, відомчих локальних обчислювальних мереж тощо. Тимчасове призупинення, дезорганізація чи ускладнення діяльності систем управління транспортом, енерго- й газопостачанням тощо. Вибіркове призупинення та порушення діяльності систем управління об'єктами критичної інфраструктури, включно з банківською сферою, підприємствами атомної, хімічної, нафтопереробної промисловості тощо
Стратегічний	Розкриття таємних кодів і шифрів, перехоплення й розшифрування листування високопосадовців. Неправомірний доступ до державних баз даних, у яких зберігається інформація з обмеженим доступом, крадіжка, редагування або знищення інформації в базах даних органів державного управління. Завдання програмної або апаратної шкоди інформаційним системам на атомних електростанціях, підприємствах хімічної, нафто і газопереробної сфери тощо. Знищення, редагування баз даних операторів стільникового зв'язку, провайдерів Інтернет, відомчих комп'ютерних мереж, систем централізованого управління енерго- і газопостачанням, зв'язком тощо
Спеціальний	Несанкціонований доступ до систем управління стратегічною зброєю та імітація примусового запуску окремих елементів ракетної чи іншої зброї. Блокування систем управління військами, передача у війська хибних наказів і директив. Дезорганізація космічного угруповання супротивника, ураження систем управління й орієнтації супутників різного призначення, переведення їх на нестабільні орбіти. Блокування запуску стратегічних та тактичних ракет, зміна їх польотного завдання й навіть перенацілювання їх на інші об'єкти в суміжних країнах тощо

У цьому випадку під кібератакою доцільно розуміти сукупність узгоджених за ціллю, змістом і часом дій (кібердій), які реалізуються в кіберпросторі та призводять або можуть

призвести до порушення конфіденційності, цілісності, доступності, спостережності та/або авторства інформації, а також порушення роботи ІТ-систем.

Під кібероперацією, за аналогією з методами звичайної війни, – вважають сукупність узгоджених за часом, глибиною та завданнями відносно короткочасних кібератак, спрямованих на один або декілька об'єктів впливу протиборчої сторони з наміром одержання незаконного доступу до їхніх інформаційних ресурсів, порушення роботи їхніх інформаційних систем або взагалі повного виведення обраних об'єктів із функціонування.

Кібероперації можуть проводитися за допомогою спеціальних засобів ураження (спеціально організованої інформації та інформаційних технологій), що становлять зміст поняття «кіберзброя» і надають змогу конкретно редагувати, копіювати, видаляти та блокувати інформацію, проникати крізь системи захисту, блокувати доступ законних користувачів, порушувати роботу носіїв інформації для дезорганізації роботи технічних засобів комп'ютерних систем та інформаційно-обчислювальних мереж. При цьому до спеціальних оборонних засобів слід віднести засоби, призначені для захисту й виявлення атак противника, а також протидію атакам.

Спеціальні оборонні засоби можуть бути поділені на такі групи:

засоби захисту інформації (засоби захисту каналів зв'язку, території, приміщень, пристроїв; засоби захисту операційних систем, баз даних і програмного забезпечення; засоби шифрування; засоби контролю й керування доступом і т. ін.);

розвідувальні засоби в кіберпросторі (радіоелектронна, кіберрозвідка та інші види розвідки).

Як одну з можливостей протистояти сучасним загрозам у сфері інформаційної та кібербезпеки британські програмісти запропонували нову оборону кіберзброю – «Інтернет-телескоп». Він відстежує проблемні зони мережі Інтернет й автоматично припиняє кібератаки [7]. Проникаючи в «глибини» мережі, «телескоп» аналізує вміст трафіку (переданих даних) на предмет наявності злоякісних програмних кодів, які призводять до перетворення окремих зон мережі на ботнети, що складаються з уражених машин – «комп'ютерів-зомбі». Уражені машини, найчастіше без відома їхніх користувачів і власників, віддалено керуються зловмисниками та втягуються у виконання масованих дій на кшталт розсилання спаму, навмисного створення надмірного числа запитів на ті чи інші сервери (DDoS-атаки) з метою спровокувати їх відмову тощо.

Виявивши заражені вузли мережі, «телескоп» встановлює фізичне місце перебування окремих «зомбованих» комп'ютерів і складає карту загроз, яка, за бажанням, може бути проаналізована фахівцями. У подальшому «телескоп» без зайвого втручання обслуговуючого персоналу визначає тип шкідливої програми й переводить її подальші дії під свій контроль.

Як заявили представники британського уряду [7], відсутність таких та подібних, «більш реалістичних» рішень, у сфері протидії кібератакам на критично важливу інфраструктуру (фінансові ринки, банківські мережі, об'єкти енергетики, телекомунікації тощо) може суттєво «підштовхнути міждержавні кібервійни в майбутньому». Аналогічну позицію висловлено в доповіді генерального секретаря Міжнародного союзу телекомунікацій Хамадуна Турі на виставці ITU Telecom World у Женеві, в якій він визначив, що «третя світова війна може початися як наслідок інформаційного протиборства саме в кіберпросторі» [8]. І тоді, за його ж словами, майже будь-яка людина «за допомогою армії заражених комп'ютерів («ботів») зможе мати велику владу у такій віртуальній битві».

Наступальна зброя кібероперацій охоплює засоби активного комп'ютерного впливу, здатні порушити функціонування інформаційних систем органів управління державних і військових об'єктів, промисловості, транспорту, зв'язку, енергетики, банків та інших установ шляхом безпосереднього інформаційного втручання в роботу комп'ютерних систем. Найчисленнішою й найнебезпечнішою для ІТ-систем противника серед наступальних засобів є група активного впливу, тобто атакуюча кіберзброя. До її арсеналу можна віднести:

комп'ютерні віруси; програмні закладки й логічні бомби; електромагнітні гармати (портативні генератори електромагнітних випромінювань великої потужності); різноманітні пристрої постановки активних комунікаційних перешкод; засоби знищення, перекручування та розкрадання інформаційних масивів; спеціальні апаратні закладні пристрої; спеціальні мікроорганізми, здатні руйнувати ізоляційний матеріал та радіоелектронні елементи.

Зазначені засоби найбільшою мірою здатні вразити найважливіші АСУ супротивника, які діють у реальному часі, наприклад, системи спостереження й попередження про ракетний напад, системи наведення зброї тощо.

Одним із доволі показових прикладів застосування атакуючої кіберзброї слід вважати події 2010 р., спричинені мережевим хробаком Win32/Stuxnet. Проникнувши в систему іранської АЕС у Бушері, вірус, розроблений групою експертів, які, найімовірніше, володіли сучасною технічною базою, загальмував ядерну програму Ірану практично без насильства.

Перш ніж потрапити до АЕС у Бушері, вірус протягом тривалого часу поширювався світом через флеш-накопичувачі за допомогою невідомої раніше уразливості ОС Windows. Як з'ясувалося, він був вузько цілеспрямованим і, згідно з опублікованими у засобах масової інформації на кшталт [9] та іншими даними, мав на меті впровадження шкідливого функціонала до промислових інформаційних систем контролю над виробничими процесами класу SCADA, що працюють під керуванням SIMATIC WinCC корпорації Siemens, проведення їх подальшого моніторингу, а також крадіжку з них інформації та змінювання реєстрів.

Як видно з наведених вище прикладів, оборонна й наступальна кіберзброя може застосовуватися переважно двома способами. Перший з них передбачає впровадження програмних та апаратних закладок у технічні засоби обробки інформації на етапі їхнього виробництва з подальшим постачанням у визначені країни (активуються ці закладки, як правило, за спеціальною командою). Другий передбачає застосування кіберзброї шляхом фізичного проникнення на об'єкт або використання спеціальних технічних засобів уже в процесі ведення кіберборотьби – комплексу заходів, спрямованих на здійснення управлінського та/або деструктивного впливу на автоматизовані ІТ-системи супротивника й захисту від такого впливу власних інформаційно-обчислювальних ресурсів шляхом використання спеціально розроблених програмно-апаратних засобів. Як стверджує директор Лондонського міжнародного інституту стратегічних досліджень Джон Чіпмен [7], імовірність застосування оборонної та наступальної кіберзброї дуже зросла, але вона й досі залишається «серйозно недооціненою» загрозою міжнародній безпеці. Як один із можливих прикладів ведення кібервоєн доцільно навести акт публікації величезної кількості конфіденційної інформації на сайті Wikileaks. Тобто в цьому випадку США виявилась, як і практично всі інші провідні країни світу, абсолютно неготовою до кібервійни, уразливою для такого роду атак і такою, що не в змозі забезпечити належний рівень захисту власних конфіденційних даних.

Так, стрімкі темпи розвитку світової науково-технічної думки та подальшого вдосконалювання ІТ-систем і технологій фактично призвели до створення єдиного глобального інформаційного й кіберпросторів, у яких у перспективі будуть акумульовані всі засоби збору, накопичення, обробки, обміну та зберігання інформації.

Це, у свою чергу, формує передумови для:

упровадження нових та розвитку існуючих форм і способів інформаційного протиборства за володіння світовим інформаційним ресурсом;

зростання ймовірності виникнення конфліктів у боротьбі за досягнення й утримання інформаційної переваги одних суб'єктів над іншими тощо.

Основною формою таких дій у недалекому майбутньому стануть, скоріш за все, кібервійни, які відрізнятимуться від звичайних бойових дій і слугуватимуть лише приводом до їх розв'язання. Їхні основні цілі, скоріш за все, полягатимуть передусім у здійсненні кіберрозвідки в органах державного та військового управління, порушенні цілісності й

доступності інформації та прозорості процесів, руйнуванні інфраструктури мереж або їхніх окремих елементів, блокуванні або виведенні з ладу автоматизованих систем управління тощо.

Основними об'єктами негативного впливу кібервійн (об'єктами критичної інформаційної інфраструктури) при цьому можуть бути:

комп'ютерні мережі державних урядових органів, фінансових установ, енергетичного сектору;

системи керування повітряним рухом, рухом залізничного транспорту та важливих підприємств, критичних для життєдіяльності;

автоматизовані системи управління військами та зброєю;

інші мережі, що призначаються для збору, обробки, збереження та видачі інформації, виведення з ладу яких також може вплинути на досягнення поставлених цілей тощо.

Тобто, якщо взяти до уваги головні характеристики майбутніх кібервоєн, а саме: можливість здійснення нападу будь-ким; географічну досяжність; невідворотність; потенціал і легкість поширення, а також вплив на «електронно готові» цілі, – можна припустити, що їхній початок може стати революцією у військовій справі, а їхні результати взагалі можуть виявитися непередбачуваними. Здебільшого це пояснюється тим, що:

кібервійна дає можливість здійснювати атаки безпрецедентній кількості аматорів, яким достатньо мати з'єднання з мережею Інтернет (вплив таких атак зростатиме з посиленням ролі глобальної мережі в щоденному політичному, соціальному й економічному житті);

кібервійна не передбачає тих витрат і зусиль, яких потребують напади на цілі, розташовані на далекій відстані (її поширення не обмежується засобами комунікації, як це було раніше);

кібервійна – це відносно легкий спосіб скористатись дедалі сильнішою залежністю від упровадження сучасних ІТ-технологій;

кібервійна не заміщає собою війну звичайну. Фактично вона є іншою ареною ведення більш масштабної війни. І ті країни, які першими оволодіють мистецтвом кібервійни, зможуть отримати фундаментальну перевагу вже на її початкових стадіях.

Висновки. За результатами викладеного матеріалу пропонується змінити прийняті в нашій державі підходи до визначень та термінологічних взаємозв'язків між кіберопераціями та кібердіями, розробити та впровадити відповідні документи та закупити новітні засоби зв'язку для розвитку новітніх ІТ-технологій країни.

Напрямки подальших досліджень. Аналіз та розробка подальших рекомендацій із удосконалення форм та способів кібердій в оборонній операції сил оборони на основі найкращих світових практик, зокрема, ґрунтуючись на керівних документах провідних країн світу та країн-членів НАТО з організації та ведення кібервійн та кібероперацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Национальная стратегия обеспечения безопасности киберпространства США: Неофиц. перевод // Смирнов А. Информационная глобализация и Россия: вызовы и возможности. М., 2005. С. 363–370.

2. Cyberwar: War in the Fifth Domain // The Economist. 2010. Jul 1st.

3. Clarke R. A. Cyber War. Harper Collins. 2010.

4. Мережко А. А. Конвенция о запрещении использования кибервойны в глобальной информационной сети информационных и вычислительных ресурсов (Интернете) // URL: http://www.politik.org.ua/vid/publcontent.php3.

5. Ляшенко І. О., Кириленко В. А. Кібернетичні операції – майбутня форма збройної боротьби // URL: http://www.nbuv.gov.ua/portal/soc_gum/znpnapv_vtn/2010_53/10liofzb.pdf.

6. СМИ внезапно вспомнили о черве WIN32/Stuxnet // URL: http://purogok.ucoz.ua/news/smi_vnezapno_vspomnili_o_cherve_win32_stuxnet/2011/09/30/501.

7. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. 2017. № 45. С. 403.

8. JP 3-12, Cyberspace Operations, 08 June 2018.

9. FM 3-12, Cyberspace and Electronic Warfare Operations, 11 April 2017.

10. NATO Standard Ajp-3.10.2 Allied Joint Doctrine For Operations Security And Deception, Edition A Version 2, January 2020.

11. NATO Standard Ajp-3.20 Allied Joint Doctrine For Cyberspace Operations, Edition A Version 1, January 2020.

12. STANAG 6514 Allied Joint Doctrine For Cyberspace Operations, Edition 1, 29 January 2020.

УДК 621.396

Плугова О. Б. ORCID: 0000-0001-7848-7806 (ВІТІ ім. Героїв Крут)
Цимбал І. В. ORCID: 0000-0001-7294-3794 (ВІТІ ім. Героїв Крут)
Яковчук О. В. ORCID: 0000-0002-6312-5009 (ВІТІ ім. Героїв Крут)

СВІТОВІ ТЕНДЕНЦІЇ ЗІ СТВОРЕННЯ ТА РОЗВИТКУ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ЗБРОЙНИМИ СИЛАМИ

Різноманітність підходів до створення автоматизованих систем управління збройними силами в різних державах створює проблему відносно найбільш доцільних підходів щодо їх створення.

Безперечно основним критерієм функціонування автоматизованих систем управління збройними силами є підвищення ефективності управління бойовими формуваннями. З урахуванням широкого впровадження процесів інформатизації, як в суспільстві, так і у військовій справі, створюються передумови розширення можливостей автоматизації управлінських процесів.

В останні десятиліття збройні сили більшості розвинених країн світу (США, держав членів НАТО, Ізраїлю) перейшли від концепції «платформоцентричної війни», при веденні якої основний акцент робився на перехід від концепції збільшення кількості й потужності озброєння та військової техніки, до концепції «мережецентричної війни». Цей перехід став результатом еволюційної зміни стратегії й тактики ведення бойових дій під впливом стрімкого розвитку військових технологій.

Концепція ведення мережецентричних бойових дій передбачає збільшення бойової потужності угруповання об'єднаних сил завдяки утворенню інформаційно-комутаційної мережі [1], що об'єднує джерела інформації (розвідки), органи управління та засоби поразки (придушення), і, таким чином, забезпечує доведення до учасників операцій достовірної та повної інформації про обставини у реальному часі.

Так, впровадження мережевих технологій у військову сферу стало революційним кроком, який спрямований на підвищення бойових можливостей збройних сил не завдяки підвищенню вогневих, маневрових та інших характеристик індивідуальних платформ озброєння, а внаслідок скорочення циклу бойового управління.

Завдання вивчення досвіду передових країн світу та їх безумовне врахування не може відкидати врахування бойового досвіду Збройних сил України, враховуючи його масштабність та комплексність застосування, практично, усіх конвенційних засобів збройної боротьби.

Ключові слова: *ефективність управління, цикл управління, підтримка прийняття рішень.*

O. Pluhova, I. Tsymbal, O. Yakovchuk A global trend in creation and development automated armed forces control systems.

The diversity of approaches to the creation of automated systems of control of armed forces in different states creates a problem regarding the most appropriate approaches to their creation.

Undoubtedly, the main criterion for the functioning of automated control systems of the Armed Forces is the improvement of the effectiveness of combat order management. Taking into account the wide implementation of informatization processes, both in society and in military affairs, prerequisites are created for expanding the possibilities of automation of management processes.

In recent decades, the armed forces of most of the developed countries of the world (the United States, NATO member states, Israel) have moved from the concept of "platform-centric warfare", during which the main emphasis was placed on the transition from the concept of increasing the number and power of weapons and military equipment, to the concept of "network-centric war ". This transition was the result of an evolutionary change in the strategy and tactics of conducting military operations under the influence of the rapid development of military technologies.

The concept of conducting Network-centric combat operations provides for an increase in the combat power of a group of joint forces due to the formation of an information and switching network [1], which unites sources of information (intelligence), control bodies and means of defeat (suppression), and thus provides evidence reliable and complete information about the situation in real time to the participants of operations.

Thus, the introduction of network technologies into the military sphere became a revolutionary step, which is aimed at increasing the combat capabilities of the armed forces not at the expense of increasing the firing, maneuvering and other characteristics of individual weapon's platforms, but at the expense of shortening the combat control cycle.

The task of studying the experience of the advanced countries of the world and its unconditional consideration cannot reject the consideration of the combat experience of the Armed Forces of Ukraine, given its scale and the complexity of using almost all conventional means of armed struggle.

Keywords: *management efficiency, management cycle, decision support.*

Постановка завдання. Побудова систем управління збройними силами з часом еволюціонує і набуває нового змісту, відповідно до розвитку як сучасних інформаційних технологій, так і засобів й способів ведення збройної боротьби.

У зв'язку з цим у наукових публікаціях та в практиці планування бойового застосування сил і засобів спостерігається потреба до постійного аналізу, оцінки можливих варіантів побудови оптимальної технічної основи системи управління військами та зброєю.

У цій публікації досліджуються основні світові тенденції зі створення та розвитку автоматизованих систем управління збройними силами, що дозволить вивчити досвід будування та застосування автоматизованих систем управління збройними силами в різних країнах, з урахуванням специфіки визначених перед ними завдань.

Актуальність викладеного матеріалу полягає в необхідності проведення постійного аналізу світових тенденцій зі створення та розвитку автоматизованих систем управління збройними силами, і як результат, постійного коригування вимог автоматизованої системи управління Збройними силами України.

Розмаїття телекомунікаційних мереж, інформаційних систем різного призначення, процесів їх руйнування та відновлення роблять проблему розробки оцінки стійкості та ефективності системи управління вкрай затребуваною під час планування та ведення бойових дій. Вирішення зазначеної проблеми полягає в створенні передумов та побудові сучасної, ефективної та стійкої автоматизованої системи управління Збройними силами України.

Аналіз останніх досліджень і публікацій. У публікації [1–3] представлено методики та принципи побудови мережецентричних систем управлінням з урахуванням загальноприйнятих в НАТО вимог, що застосовуються для аналізу структурованих мереж, в яких враховується їх зв'язність.

У публікації [4] викладено основні ознаки ведення мережецентричних війн сучасності, з аналізом та поглядами щодо побудови відповідних мережецентричних систем управління. Однак, враховуючи стрімкий розвиток технологій, певні положення, що викладені, потребують уточнення.

У публікації [5] окреслено перспективи розвитку автоматизованих систем управління тактичної ланки управління Сухопутних військ Збройних сил України. З урахуванням досвіду російсько-української війни та інших збройних конфліктів сучасності необхідно комплексне бачення завдань та вимог до сучасних автоматизованих систем управління збройними силами.

Метою статті в умовах застосування в Збройних силах України різноманітних інформаційних систем та їхніх елементів є проведення аналізу світових тенденцій зі створення та розвитку автоматизованих систем управління збройними силами та вивчення досвіду передових країн світу.

Виклад основного матеріалу. Аналіз основних напрямків та сучасних світових тенденцій зі створення автоматизованих систем управління збройними силами свідчить, що в провідних західних державах на сьогодні першочергова увага приділяється питанню підвищення ефективності управління бойовими формуваннями. З поглибленням процесів інформатизації, як суспільства, так і військових формувань, створилися передумови розширення можливостей автоматизації управлінських процесів.

У сучасних умовах високий рівень інформаційного забезпечення бойових дій військ стає визначальною умовою досягнення як стратегічної та оперативно-тактичної, так за певних умов і тактичної переваги над супротивником. Вирішальним фактором успіху стала здатність проводити мережецентричні операції, у яких висока ефективність командування й управління забезпечується можливостями обчислювальної техніки, засобів зв'язку й розвідки (C4ISR – Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance). Зважаючи на досвід ведення бойових дій Збройних сил України у вітчизняній війні з російськими загарбниками, саме широке впровадження інформаційних технологій

(в деяких випадках, їхніх елементів) та наявність практичного досвіду застосування надають переваги в скороченому циклі управління військами та бойовими засобами.

Військовими фахівцями провідних країн світу (США, Європейських держав, Ізраїлю) постійно та активно проводяться роботи із забезпечення якісно нового рівня інформаційної сумісності систем розвідки, спостереження, навігації, управління й ударних комплексів (засобів) у рамках побудови єдиної для всіх видів і родів військ інформаційно-управляючої інфраструктури. Її технічною основою буде виступати глобальна (просторово-рознесена) інформаційна мережа, створена на базі наявних і перспективних мереж зв'язку й передачі даних на основі застосування сучасних Інтернет-технологій, що володіє високими оперативно-технічними характеристиками.

У сучасній війні для забезпечення ефективної управлінської діяльності характерним стає вирішення поставлених задач у реальному масштабі часу або близькому до реального, яке забезпечується широким впровадженням комп'ютерної техніки, різних електронних баз (банків) даних, комплексів прикладних програм, представлення даних у формі зображень, документообіг в електронному виді, застосування цифрових карт і відеозображень місцевості. Крім того, посадовими особами органів військового управління все активніше використовуються інформаційні засоби підтримки прийняття рішень, різні комп'ютерні моделі для оцінки обстановки, а також перевірки і вибору раціонального варіанта рішення під час планування бойових дій.

Наслідком цього є посилення залежності системи управління від її технологічної складової, основу якої утворюють система зв'язку й системи та комплекси засобів автоматизованого управління військами й зброєю.

В останні десятиліття збройні сили більшості розвинених країн світу (США, держав членів НАТО, Ізраїлю) перейшли від концепції «платформоцентричної війни», при веденні якої основний акцент робився на перехід від концепції збільшення кількості й потужності озброєння та військової техніки, до концепції «мережецентричної війни». Цей перехід став результатом еволюційної зміни стратегії й тактики ведення бойових дій під впливом стрімкого розвитку військових технологій.

Основною ідеєю та ведення «мережецентричної війни» є інтеграція всіх сил і засобів у єдиний інформаційний простір, що дозволяє багаторазово збільшити ефективність їх бойового застосування завдяки швидкому прийняттю управлінських рішень та наявності з ними постійного зворотного зв'язку. Отже, впровадження мережевих технологій у військову сферу стало революційним кроком, який спрямований на підвищення бойових можливостей збройних сил не через підвищення вогневих, маневрових та інших характеристик індивідуальних платформ озброєння, а внаслідок скорочення циклу бойового управління.

Згідно з висновками іноземних експертів перевага над противником досягається шляхом істотного поліпшення якості управління – повноти, глибини знань, єдиного розуміння й оцінки обстановки, що динамічно розвивається, командуванням усіх рівнів, своєчасного реагування і прийняття обґрунтованих рішень, прискореного доведення їх до діючих сил для реалізації.

Мережецентрична війна — війна, орієнтована на досягнення інформаційної переваги за допомогою об'єднання військових об'єктів у інформаційну мережу. Її визначення можна окреслити відповідною концепцією та принципами ведення такої війни.

Концепція ведення Мережецентричних бойових дій, передбачає збільшення бойової потужності угруповання об'єднаних сил завдяки утворенню інформаційно-комутаційної мережі [1], що об'єднує джерела інформації (розвідки), органи управління та засоби поразки (придушення), що забезпечує доведення до учасників операцій достовірної та повної інформації про обставини у реальному часі.

Внаслідок досягається прискорення управління силами та засобами, підвищення темпу операцій, ефективності поразки сил противника, живучості своїх військ та рівня самосинхронізації бойових дій [1].

Мережецентричні сили у військовому сенсі — це війська та зброя, здатні реалізувати концепцію мережецентричної війни.

Концепція передбачає переклад переваг, властивих окремим інфокомунікаційним технологіям в конкурентну перевагу рахунок об'єднання у стійку мережу інформаційно досить добре забезпечених, географічно розосереджених сил. Ця мережа, поєднана з новими технологіями та новим рівнем організації процесів та людей, передбачає нові форми організаційної поведінки.

Теорія мережецентричної війни містить у основі три принципи [1]:

1. Сили, об'єднані досить надійними мережами, набувають можливість якісно нового обміну інформацією та досягнення інформаційної переваги над противником.
2. Обмін інформацією підвищує якість інформації та рівень загальної поінформованості про те, що відбувається.
3. В результаті загальна ситуаційна поінформованість така, що дозволяє забезпечувати необхідну співпрацю та самосинхронізацію, підвищує стійкість та швидкість передачі команд, що, у свою чергу, різко підвищує ефективність виконання бойового завдання.

«Мережецентрична війна» може здійснюватися на всіх рівнях військових дій – тактичному, оперативному й стратегічному. Принципи її ведення жодним чином не залежать від географічного регіону, бойових задач, складу та структури задіяних військ.

Одним з основних елементів проведення «мережецентричних операцій» є система автоматизованого управління військами та зброєю, яка на сучасному етапі розглядається в рамках структури C5ISR (Command, Control, Communications, Computers, Combat Systems, Intelligence, Surveillance and Reconnaissance – Бойові системи, системи керування, зв'язку, комп'ютерного забезпечення, розвідки й спостереження).

У зв'язку з розвитком інформаційних технологій, у світі розпочата світова «мережецентрична гонка». Зокрема, НАТО реалізує концепцію «Комплексні мережеві можливості» (NATO Network Enabled Capabilities), Франція – «Інформаційно-центрична війна» (Guerre Infocentre), Швеція – «Мережева оборона» (Network Based Defense), КНР – «Система бойового управління, зв'язку, обчислювальної техніки, розвідки й вогневого знищення» (Command, Control, Communications, Computers, Intelligence, Surveillance, Recognizance&Kill), Ізраїль – програма «Цифрова армія», Нідерланди – «Мережецентричні операції» (Network Centric Operation), Великобританія – «Мережеві можливості» (Network Enabled Capability), Австралія – «Мережецентрична війна» (Network Centric Warfare).

Саме в «мережецентризмі» військові експерти розвинутих країн вбачають дієвий інноваційний інструмент підвищення бойових можливостей збройних сил. Згідно з їхніми прогнозами збройні сили провідних держав переходять із 2020 року від «платформоцентричних» до «мережоцентричних» принципів проведення операцій.

Якщо подивитися на тенденції, виходячи з даних аналітичного прогнозу – «The C2/C4 ISR Market Analysis, Financials and Forecasting 2010–2020» (агентство ASD Repports), обсяг ринку інформаційних систем у 2010 році склав 63,6 млрд дол. США, що становить близько 5 % від світового обсягу оборонних витрат. При цьому, країни Африки і пострадянського простору практично не були задіяні, а потенційна ємність їхнього ринку (без РФ), складає близько 500 млн дол. США на рік.

У період з 2020 р. до 2025 р. прогнозується зростання попиту на інформаційні системи C2/C4ISR (Command and Control/Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) у регіонах, що раніше не проявляли активності у зазначеному сегменті, де привабливими ринками можуть стати країни Африки, Південної Америки, Азіатсько-Тихоокеанського регіону та держави пострадянського простору.

Крім військових замовників, інтерес до систем подібних С2/С4ISR проявляють цивільні служби (МНС, поліція, рятувальні служби, охоронні підрозділи), що активно використовують інформаційні системи в процесах управління й всебічного забезпечення.

США. Наприкінці 90-х років XX століття військове керівництво США визначило реалізацію концепції ведення військових дій у єдиному інформаційному просторі або з використанням об'єднаних інформаційно-управляючих мереж (NCW – Network-Centric Warfare) [1] як одного з основних напрямків своєї діяльності з підвищення бойових можливостей об'єднаних збройних сил і підготовці їх до спільних операцій в XXI ст.

Відповідно до цієї концепції передбачається за допомогою впровадження у війська передових інформаційних технологій (високопродуктивних комп'ютерів, сучасного програмного забезпечення, цифрових швидкісних систем передачі даних) поєднати розосереджені у великому бойовому просторі різнорідні сили й засоби (особовий склад; органи й пункти управління, бойового забезпечення; озброєння й військову техніку наземного, повітряного й морського базування) у формування з високою мережевою архітектурою – глобальні й локальні інформаційні мережі.

Концепція «мережецентричної війни» означає перетворення Збройних сил США в гігантський розвідувальний і ударний комплекс, що перебуває в єдиному інформаційному просторі. Так, для Міністерства оборони США розробка нових підходів до командування й управління (Command&Control – C2) є ключовим напрямком модернізації національної системи безпеки.

У рамках «Єдиної мережі Збройних сил» функціонує «Об'єднана система бойового управління та зв'язку» (Joint Battle Management Command and Control – JBMC2), яка формується під контролем Міністерства оборони США з метою забезпечення своєчасного доведення необхідної інформації до зацікавлених споживачів у прийнятному для використання форматі. «Серцем» мережі повинне стати Сімейство (сукупність) взаємозалежних даних про хід та розвиток подій (Family of Interoperable Operation Pictures – FIOP). До складу такого сімейства увійдуть дані про обстановку повітряного, наземного, морського й космічного простору.

З метою реалізації стратегії розвитку збройних сил у США розгорнуто програму Future Combat Systems (FCS), яка являє собою систему автоматичних роботизованих бойових машин, зв'язаних між собою, а також з командними пунктами за допомогою високошвидкісних каналів зв'язку. В узагальнену систему управління боєм включені солдати, літаки та БПЛА, танки й бронетранспортери, пускові ракетні установки, а також супутникові системи. В результаті АСУ забезпечує безперервність і швидкість процесів управління від стратегічної ланки аж до окремого солдата. За оцінками фахівців вартість такого проєкту становитиме до 500 млрд дол. США.

У рамках реалізації програми FCS та створення ЄАСУ Міністерством оборони США створюються системи С4ISR, які постійно тестуються та вдосконалюються під час ведення бойових дій в локальних конфліктах:

– TBMCS (Theater Battle Management Core Systems) – система бойового планування й управління авіацією на театрі бойових дій;

– FBCB2 (Force XXI Battle Comm and Brigade or Below) – інформаційна система бойового управління, що охоплює рівень «бригада – батальйон – рота»;

– MTC (Army's Movement Tracing System) – система адресного тилового забезпечення;

– CAC2S (Marine Corps Common Aviation Command and Control System) – система управління, контролю й координування повітряними операціями морської піхоти та інші.

Нині США є безперечним лідером у створенні ЄАСУ та проведенні військових операцій за мережецентричними принципами.

НАТО. Основні підходи до використання нових технологічних досягнень в інтересах об'єднаних військових сил НАТО викладено в концепції єдиного інформаційного простору

альянсу NNEC (NATO Network Enabled Capability) [2], за основу якої взята аналогічна американська концепція NCW (Network-Centric Warfare). Концепція єдиного інформаційного простору передбачає створення глобального інформаційного середовища, що забезпечує комплексну обробку відомостей у реальному масштабі часу про супротивника, свої війська й навколишню місцевість в інтересах підтримки прийняття рішення щодо створення угруповань військ оптимального (для досягнення поставлених цілей) складу і їх ефективного використання в різних умовах.

Нині затверджено єдину інформаційну модель JC3IEDM (Joint Command, Control and Consultation Information Exchange Data Model, Об'єднаного командування, управління і консультацій обміном інформацією) [3], яка є стандартом для всіх інформаційних систем країн НАТО. Інформаційна модель розвивається в рамках програми всебічної сумісності інформаційних систем НАТО – MIP (багатостороння програма взаємодії) [3].

Інтеграцію автоматизованих інформаційно-управляючих систем альянсу планується здійснити в рамках програми A4ISR, яка передбачає об'єднання систем обробки даних стосовно противника і своїх військ в єдиний інформаційний простір блоку для формування командної й аналітичної основи АСУ.

З урахуванням організаційної і технічної складності реалізації концепції єдиного інформаційного простору НАТО, досягнення повної оперативної готовності планується в 2020–2025 роках.

Командування об'єднаних збройних сил НАТО з питань трансформації NATO's Allied Command Transformation (ACT) обрало компанію «IBM» (США) для реалізації стратегічного технологічного проєкту з узагальнення та практичного впровадження досвіду застосування нових інформаційних технологій, підвищення ефективності центрів обробки даних і забезпечення доступу до загальних інформаційних ресурсів усіх 28 членів Альянсу. Проєкт дозволить консолідувати й інтегрувати технологічні можливості систем управління класу С2 (Command&Control).

Китайська Народна Республіка. КНР неухильно і постійно збільшує військові витрати. За офіційними даними оборонний бюджет за останні вісім років збільшився у чотири рази. Однак, експерти вважають, що офіційні військові витрати КНР занижені у 1,5–3 рази.

Держава подолала технологічне відставання і швидкими темпами модернізує свої збройні сили. Зокрема, здійснюються заходи щодо реалізації концепції «Система бойового управління, зв'язку, обчислювальної техніки, розвідки й вогневого знищення» (Command, Control, Communications, Computers, Intelligence, Surveillance, Recognizance&Kill). За оцінками фахівців Пекін створить сучасну армію до 2020–2025 року.

Зусилля військово-політичного керівництва КНР спрямовані на те, щоб «всередині» Народно-визвольної армії Китаю (НВАК) з'явилася відносно невелика (15 % від загальної чисельності збройних сил у мирний час) сучасна високотехнологічна армія, здатна успішно протистояти збройним силам, зокрема США, РФ, Японії та Індії, а також будь-якій іншій державі. Для цієї армії будуть максимально враховуватися новітні американські концепції військового будівництва – концепція «мережецентричної війни».

Однак, значна увага приділена «асиметричній війні» – впливу на «нервові вузли» ворожої армії (електронне й вогневе виведення з ладу командних пунктів, космічних апаратів, центрів зв'язку противника, а також заходи щодо дезінформації й маскування). З цією метою активно створюються підрозділи «хакерів». У 2000 році мережеві війська стали окремим родом військ НВАК.

Ізраїль. Digital army program (DAP) – інвестиційна програма, підписана між Міністерством Оборони Ізраїлю та компанією «Elbit Systems» в 2004 році, головна мета якої створення єдиного інформаційного простору в цифровій формі, що дає можливість взаємодіяти наземним, повітряним і морським підрозділам через захищений широкосмуговий зв'язок.

Згідно з контрактом у війська будуть поставлені апаратні та програмні засоби, включно зі станціями командування й управління, системи обробки і розподілу даних. Програма передбачає забезпечення зв'язком датчики і засоби ведення вогню на всіх командних рівнях, забезпечення координації військ, доступ до ситуаційних сценаріїв, що регулярно оновлюються, удосконалення оперативних можливостей, у тому числі забезпечення живучості й точності, більш ефективне використання особового складу й інших ресурсів.

Як одна зі складових програми DAP, в армії Ізраїлю впроваджують систему «Fast Road» – нове покоління технологій побудови автоматизованих систем управління боєм для танкових підрозділів. Технологічні рішення, застосовані в системі «Fast Road», забезпечують високу швидкість обміну інформацією й дозволяють обновляти відображення обставин і командної інформації в реальному масштабі часу.

Отже, як можна побачити, провідні країни світу демонструють чудовий приклад, як швидко розвивати інноваційні технології та доводити їх до військ.

Зокрема, на прикладі США проглядається свідоме розуміння необхідності змін для утримання інноваційного лідерства у сфері національної безпеки. Майже кожне силове відомство має для цього відповідні ресурси. Наприклад, Агентство передових оборонних дослідницьких проєктів (Defense Advanced Research Projects Agency – DARPA) в системі Міністерства оборони США, Агентство передових дослідницьких проєктів у сфері розвідки (Intelligence Advanced Research Projects Activity – IARPA), підпорядковане директору Національної розвідки США, її аналог (Homel and Security Advanced Research Projects Agency – HSARPA) Міністерства внутрішньої безпеки США.

Одним із найбільш актуальних і пріоритетних напрямків удосконалення систем управління військами і зброєю у Збройних силах провідних країн світу є забезпечення їх тісної інтеграції із засобами зв'язку, розвідки і ураження за допомогою формування єдиного інформаційного простору (ЄІП) для всіх учасників операції (бойових дій). При цьому в інформаційній взаємодії беруть участь всі – від солдата на полі бою, який забезпечується всією необхідною візуальною, географічною, тактичною й іншою інформацією, до штабів різних ланок управління.

В основі такого підходу до організації і ведення бойових дій лежить високий рівень оперативності, достовірності і повноти розвідувально-інформаційного забезпечення систем та засобів управління військами і зброєю, що й створює передумови досягнення інформаційної, а разом з тим, і повної переваги над противником [4; 5].

Висновки. Як висновок слід зазначити, що прискіпливе вивчення досвіду передових країн світу та безумовне врахування бойового досвіду Збройних сил України, усунення і подолання всіх причин і їхніх наслідків щодо вдосконалення системи управління військами в попередні роки дозволить нам якнайшвидше просунутись вперед у напрямку побудови ЄАСУ.

Шляхи майбутніх досліджень. Враховуючи швидкоплинне змінення форм і методів збройної боротьби та вплив бурхливого розвитку інформаційних технологій, постає завдання проведення постійного аналізу та прогнозування розвитку організаційної побудови військ (сил) та їхніх дій. Російсько-Українська війна є безперечно найбільшим та наймасштабнішим збройним конфліктом сучасності після закінчення Другої світової війни. Широкомасштабне застосування високоточних та високотехнологічних засобів (БпЛА різного призначення, крилаті та балістичні ракети, сучасна реактивна артилерія і т. ін.) та водночас артилерійських систем і бронетехніки часів Холодної війни створюють унікальну картину застосування зброї декількох поколінь. Така ситуація безумовно потребує подальших досліджень з огляду виконання завдання щодо підвищення ефективності управління «змішаними» угрупуваннями військ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. NETWORK CENTRIC WARFARE: Developing and Leveraging Information Superiority, (2nd Edition), David S. Alberts, John J. Garstka, Frederick P. Stein.

2. NATO NETWORK ENABLED CAPABILITY FEASIBILITY STUDY EXECUTIVE SUMMARY, VERSION 2.0, T. Buckman, Communications and Information Systems Division, 2005.

3. NATO – STANAG 5525, Joint C3 Information Exchange DataModel - JC3IEDM, Multilateral Interoperability Programme.

4. Кучеренко Ю. Ф. Головні ознаки ведення мережецентричних війн сучасності / Ю. Ф. Кучеренко // Системи управління, навігації та зв'язку. Київ: ДП «Центральний науково-дослідний інститут навігації і управління», 2011. № 1 (17). С. 190–193.

5. Лаврут О. О., Климович О. К., Лаврут Т. В. Перспективи розвитку автоматизованих систем управління тактичної ланки управління Сухопутних військ Збройних Сил України // Системи обробки інформації. Харків, 2014. Вип. 5 (121). С. 116–120.

УДК 621.391

Прохорський С. І. ORCID: 0000-0002-6369-2601 (ВІТІ ім. Героїв Крут)
Бондаренко О. Є. ORCID: 0000-0002-9123-7462 (ВІТІ ім. Героїв Крут)
Сергієнко А. В. ORCID: 0000-0001-5336-2089 (ВІТІ ім. Героїв Крут)

АНАЛІЗ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ ТА КОМП'ЮТЕРНИХ АТАК

У статті проведено аналіз проєктування системи виявлення атак, розглянуто основні принципи створення засобів виявлення і протидії комп'ютерним атакам, приведено опис застосовуваних під час виявлення та запобігання мережевих атак методи і моделі, надано характеристики моделям виявлення вторгнень.

Із розвитком цифрових технологій суттєво підвищились вимоги до системи виявлення вторгнень та комп'ютерних атак, а також до документів, які беруть участь у роботі даної системи.

Авторами даної статті зазначається необхідність розроблення та впровадження у дію законодавчого документу «Про настання відповідальності за реалізацію комп'ютерних атак та вторгнень» та постійного його наповнення.

Проведено аналіз засобів мережевого захисту, аналіз параметрів та характеристик захищеної інформаційної системи.

Розглянуто основні принципи створення засобів виявлення і протидії комп'ютерним атакам: принцип прозорості, принцип оптимальності, принцип адекватності, принцип повноти, принцип адаптивності.

Найважливішим фактором залишається стійкість системи виявлення вторгнень та комп'ютерних атак.

Напрямом подальших досліджень є вирішення проблемних питань стосовно складності об'єднання усіх принципів створення систем виявлення і протидії атакам до однієї системи, досліджень переліку загроз та класифікації видів атак.

Метою статті є визначення проблемних питань при проведенні заходів з проєктування системи виявлення вторгнень, тестування розробленого програмного засобу, виявлення та усунення його недоліків, зведення методик виявлення мережевих атак до єдиного критерію, наприклад, таким як повнота охоплення всіх аналізованих параметрів, необхідних для точного і найбільш ймовірного виявлення атаки з мінімально хибним спрацьовуванням.

Ключові слова: *комп'ютерна атака, інформаційна система, захищеність, стійкість, протидія, принцип.*

S. Prokhorskyi, O. Bondarenko, A Serhiienko Analysis of the intrusion detection system and computer attacks.

In the article researched analysis of projection system of detection of attacks is considered, basic principles of creation means detection and counteraction to the computer attacks, description is given methods and models which used for detection and counter action networ attacks, given characteristics of models of the intrusion detection.

With the development of digital technologies, the requirements for the system for detecting intrusions and computer attacks, as well as for the documents involved in the work of this system, have significantly increased.

The authors of this article note the need to develop and implement a legislative document on "On the onset of liability for the implementation of computer attacks and intrusions" and its constant filling.

Analysis of network protection means, analysis of parameters and characteristics of the protected information system was carried out.

The main principles of creating means of detecting and countering computer attacks are considered: the principle of transparency, the principle of optimality, the principle of adequacy, the principle of completeness, the principle of adaptability.

The direction of further research is to solve problematic issues regarding to the difficulty of combining all the principles of creating systems for detecting and countering attacks into one system, researching the list of threats and classifying types of attacks.

The most important factor remains the resilience of the intrusion detection system and computer attacks.

The purpose of the article is to identify problematic issues when conducting measures to design an intrusion detection system, test the developed software tool, identify and eliminate its shortcomings, reduce network attack detection methods to a single criterion, for example, such as complete coverage of all analyzed parameters necessary for accurate and most possible detection of an attack with minimal false activation.

Keywords: *computer attack, information system, security, stability, counter action, principle.*

Постановка у загальному вигляді. Як відомо, навіть найнадійніші системи захисту не здатні захистити від атак комп'ютерні системи державних та відомчих установ. Одна з причин у тому, що в більшості систем безпеки застосовують стандартні механізми захисту:

ідентифікацію та автентифікацію, механізми обмеження доступу до інформації згідно з правами суб'єкта і криптографічні механізми. Це традиційний підхід зі своїми недоліками, як-то: незахищеність від власних користувачів – зловмисників, розмитість поділу суб'єктів системи на «своїх» і «чужих» через глобалізацію інформаційних ресурсів, порівняна легкість підбору паролів внаслідок використання їхнього змістового різновиду, зниження продуктивності і ускладнення інформаційних комунікацій внаслідок обмеження доступу до ресурсів організації. Важливо, щоб такі системи могли протистояти атакам, навіть якщо зловмисник уже був автентифікований та авторизований і з формальної точки зору додержання прав доступу мав необхідні повноваження на свої дії.

Ці функції і виконують системи виявлення вторгнень (Intrusion Detection Systems, *IDS*). Оскільки передбачити всі сценарії розгортання подій в системі з активним «чужим» суб'єктом неможливо, слід або якомога детальніше описати можливі «зловмисні» сценарії або ж, навпаки, –«нормальні» і постулювати, що всяка активність, яка не підпадає під прийняте розуміння «нормальності», є небезпечною.

Аналіз останніх публікацій. Завданнями в системі виявлення вторгнень є [10]:

забезпечення виконання послуг конфіденційності, цілісності, доступності та спостережності інформації;

дослідження технології обробки інформації з метою виявлення можливих каналів витоку та інших загроз для безпеки інформації;

дотримання вимог політики безпеки інформації, проведення заходів, спрямованих на її реалізацію;

розроблення нормативних і розпорядчих документів;

участь в організації професійної підготовки і підвищенні кваліфікації персоналу

Мета. Визначення проблемних питань при проведенні заходів із проєктування системи виявлення вторгнень, тестування розробленого програмного засобу, виявлення та усунення його недоліків, зведення методик виявлення мережевих атак до єдиного критерію, наприклад, таким як повнота охоплення всіх аналізованих параметрів, необхідних для точного і найбільш ймовірного виявлення атаки з мінімально хибним спрацьовуванням.

Виклад основного матеріалу дослідження. Проведений аналіз свідчить, що *IDS* поділяються на системи, що реагують на відомі атаки – системи виявлення зловживань (Misuse Detection Systems, *MDS*) і системи виявлення аномалій (Anomaly Detection Systems, *ADS*), які реєструють відхилення еволюції системи від нормального перебігу.

Моделі виявлення і запобігання мережевих атак (МА) діляться на два типи:

хостова (*host-based*) модель виявлення МА передбачає аналіз даних, одержуваних і переданих в мережу, і аналіз різних журналів реєстрації, наявних на конкретному вузлі (хості) шляхом застосування відповідних методик і алгоритмів;

мережева (*network-based*) модель виявлення МА передбачає аналіз мережевого трафіку безпосередньо в мережі, тобто аналізуються дані, взяті з технічних каналів зв'язку, з використанням середовища передачі даних і каналоутворюючого обладнання обчислювальної мережі, шляхом застосування відповідних методик і алгоритмів мережевого аналізу даних.

Засобами технології виявлення МА є програмні та апаратні системи виявлення атак, які функціонують переважно в *TCP/IP*-мережах і базуються на сигнатурних та статистичних методиках виявлення на основі хостових і мережевих моделей.

Виявлення атак вимагає виконання однієї з двох умов: або розуміння очікуваного поведінки контрольованого об'єкта системи, або знання всіх можливих атак і їхніх модифікацій. У першому випадку використовується технологія виявлення аномальної поведінки (*anomaly detection*), а в другому – технологія виявлення зловмисної поведінки або зловживань (*misuse detection*).

Серед відомих методів виділяються наступні:

– статистичний метод;
– приховані марківські моделі;
– нечітка логіка;
– експертні системи;
– використання прогнозованих шаблонів;
– генетичні алгоритми;
– штучні нейронні мережі;
– аналіз переходів зі стану в стан;
– *data mining*-методи.

Застосовувані при виявленні та запобіганні МА методи і моделі зводяться до мережевого і хостового аналізу сигнатурних і статистичних даних мережевого трафіку з подальшим виведенням засобів виявлення атак про здійснення атаки. До таких висновків відносяться повідомлення на консоль або в журнали засобів виявлення атак про час виявлення і проведення, назву та типи атаки. Результатами роботи засобів виявлення атак є дані про номери пакетів, що містяться в сеансі атаки.

Сигнатурний аналіз і контроль профілів при виявленні комп'ютерних атак (КА) містить аналіз заданих заздалегідь послідовностей, як самих аналізованих даних, так і послідовностей дій. Сучасні методики виявлення МА досить різнорідні і не зведені до єдиного критерію, за яким можливо оцінювати ефективність їх застосування. Таким критерієм може служити повнота охоплення всіх аналізованих параметрів, необхідних для точного і найбільш ймовірного виявлення атаки з мінімально хибним спрацьовуванням.

Недоліками розглянутих моделей є: для моделей, які використовують статистичні методики, – велика кількість помилкових тривог і помилок другого роду, для моделей, що використовують сигнатурні методики, – неможливість самостійного виявлення нових атак і постійна необхідність оновлення бази сигнатур.

Під час виявлення та запобігання МА вже використовуються методики, що мають можливість саме запобігання МА і охоплюють лише такі дії, як блокування прийому/передачі тих мережевих пакетів, які ідентифікуються як пакети, що містяться в атаці.

Методики виявлення і запобігання зводяться до застосування технологій виявлення МА, які містять програмні та апаратні системи виявлення атак, функціонуючі переважно в *TCP/IP*-мережах і базуються на сигнатурних та статистичних методиках виявлення атак, на основі хостових і мережевих моделей, результатом яких є виявлення атак з метою автоматизації забезпечення захисту локальної обчислювальної мережі (ЛОМ).

У таких методиках спільною рисою з формальної точки зору є те, що існує кілька підходів подання повідомлень про виявлені атаки.

При виявленні МА переважно застосовуються методики, узагальнення приватних рішень яких будуються з використанням різноманітних методів і технологій. Найбільш відповідні області застосування методики:

– класичні методи експертних систем;
– нейронні мережі;
– нечітка логіка;
– візуалізація;
– статистика;
– *k*-найближчий сусід (метод з теорії розпізнавання);
– метод аналізу ієрархій.

Для того, щоб система прийняття рішень могла узагальнювати дані, отримані від різних підсистем системи виявлення вторгнень, необхідно стандартизувати формат повідомлень про атаки, що посилаються цими аналізаторами. Підсистема системи виявлення вторгнень повинна передавати в СПР вектор виду (1):

$$S = (A, C, G, T, M, P, P_i, P_a), \quad (1)$$

де A – системний ідентифікатор виявника атаки;

C – ідентифікатор виявленої атаки;

G – вид атаки;

T – системний час атаки;

M – ідентифікатор методу, яким виявлена атака;

P – вірогідність проведення атаки;

$P_н$ – нижня межа ймовірності атаки;

$P_в$ – верхня межа ймовірності атаки.

Подальша обробка проводиться роздільно для кожного з видів атак. Тимчасова вісь t розбивається на інтервали аналізу Δt. Довжина інтервалу Δt визначається, виходячи з типу атаки і швидкості її виявлення підсистемами СВВ. У кожному інтервалі проводиться аналіз повідомлень з метою оцінки узагальненої ймовірності атаки. У ряді робіт, виконаних у суміжних областях, показано, що вироблення оптимального методу об'єднання статистичних гіпотез про виявлення різнорідних об'єктів у практичній ситуації неможлива. Для систем виявлення атак це пояснюється відсутністю даних про апріорні ймовірності атак різних видів, різною природою проаналізованих ознак, неможливістю оцінки спільних рис розподілу значень цих ознак, рознесенням у часі моментів повідомлень про атаки.

Збільшення ймовірності виявлення атаки веде до зростання ймовірності «помилкової тривоги». Для того щоб ймовірність «помилкової тривоги» залишалася в допустимих межах, пропонується використовувати мажоритарний критерій для прийняття рішень. Якщо в системі присутні кілька виявників атак, які виявлятимуть заданий вид атаки, то рішення про наявність атаки приймається в випадку, якщо вона виявлена більш ніж половиною СВА.

Розвитком мажоритарного підходу є вимоги трудомісткої експертної роботи та застосування при обчисленні ймовірності атаки апріорної інформації про властивості підсистем, які реалізуються на основі обчислення зваженої суми значень P_i, де в якості ваги застосовується ступінь довіри до того чи іншого виявника (підсистемі СВВ) при розгляді даної конкретної атаки. Тоді ймовірність виявлення атаки (класу або групи атак) k може бути представлена виразом (2):

$$P_{\hat{E}\hat{I}\acute{A}}\left(\Delta t_i\right) = \sum_{j=1}^{m} W_{kj} \cdot P_{kj}, \tag{2}$$

де m – число аналізаторів, що використовуються в СВВ;

P_{kj} – ймовірність атаки k, передана j-м аналізатором на інтервалі Δt_i;

W_{kj} – ступінь довіри результатам роботи аналізатора j при виявленні атаки k, причому $\sum_{j=1}^{m} W_{kj} = 1$.

Якщо повідомлень про атаки в інтервалі аналізу Δt_i не зафіксовано, $P_{\hat{E}\hat{I}\acute{A}}\left(\Delta t_i\right) = 0$.

Відповідно застосування ймовірнісної оцінки виявлення атак залежить від числа аналізаторів, ймовірності атаки і ступеня довіри аналізаторам при виявленні атаки.

Сучасні засоби захисту можна розділити за характеристиками, що представлені на рисунку 1.

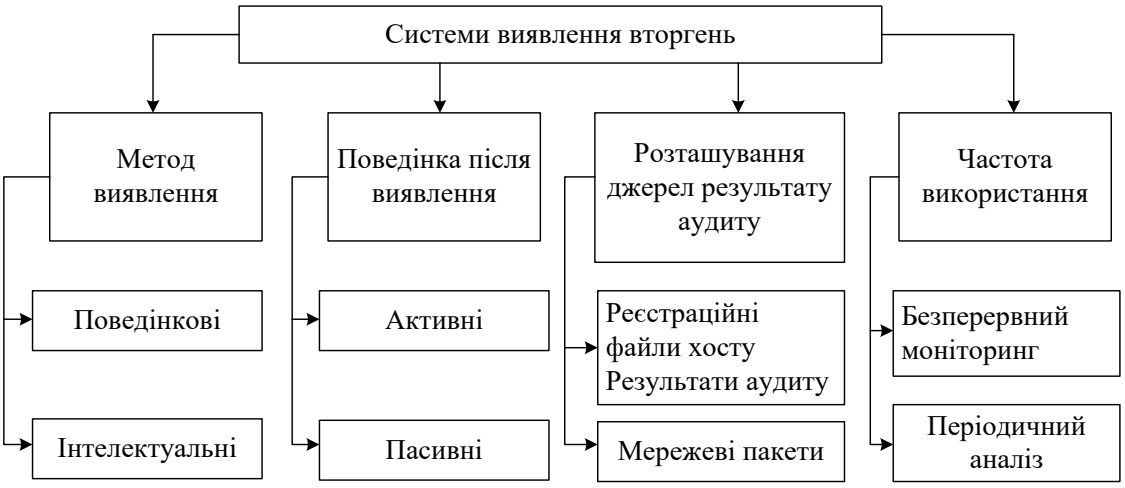

Рис. 1. Алгоритм методики виявлення вторгнень

Основними принципами створення засобів виявлення і протидії КА є такі:

1. Принцип прозорості. Система виявлення та протидії КА повинна функціонувати у фоновому режимі непомітно для користувачів, не знижуючи оперативності виконання технологічних циклів управління, при цьому забезпечуючи виконання своїх цільових функцій.

2. Принцип оптимальності. Розробка системи виявлення та протидії КА повинна проводитися з урахуванням того, що кожен з методів виявлення (протидії) КА дозволяє досить ефективно і достовірно виявляти (нейтралізувати) тільки певні види КА. Тому при створенні системи виявлення та протидії КА повинно бути знайдено оптимальне співвідношення між методами виявлення і протидії КА і способами їхнього застосування в складі системи.

3. Принцип адекватності. Розробляються для реалізації в системі виявлення та протидії КА проєктні рішення повинні бути диференційовані залежно від частоти, ймовірності та очікуваного збитку від успішної реалізації кожного виду КА.

4. Принцип повноти. Даний принцип полягає у використанні для виявлення КА інформації про стан і значення основних параметрів всіх програмних і технічних елементів пунктів управління АС.

5. Принцип адаптивності. Система виявлення та протидії КА повинна створюватися з урахуванням того, що з розвитком АС здійснюватиметься поступова зміна складу і характеристик програмних і технічних засобів АС, що, своєю чергою, призведе до розширення переліку загроз безпеки. Тому при створенні системи виявлення та протидії КА в її складі повинні бути передбачені механізми адаптації системи до мінливих умов функціонування.

Аналіз засобів мережевого захисту.

Розміщення всередині однієї ЛОМ здійснюється наступним чином. СВА розміщують так, щоб вона могла спостерігати за всіма підконтрольними їй сегментами мережі. Як правило, безпосереднє спостереження здійснюють кілька розташованих у ній сенсорів.

Сенсорами можуть бути як мережеві інтерфейси, так і групи мережевих інтерфейсів під управлінням операційної системи (наприклад, кластер *NIDS*). У самому простому випадку *IDS* встановлюють на вхід сегмента, яких захищають так, щоб весь трафік сегмента проходив через систему.

У цього варіанта є свої плюси і мінуси. До перших можна віднести:

відсутність трафіку, що не проходить через *IDS*, що знижує ймовірність непоміченого попадання зловмисного трафіку в сегмент;

можливість установки системи активного реагування на атаку (наприклад, комбінація *Snort + Guardian* дозволяє змінювати правила *ipchains /iptables* відповідно з подіями *IDS*).

До числа недоліків відносять:

появу додаткової ланки, вихід якої з ладу може позначитися на працездатності мережі в цілому;

складність масштабування *IDS* внаслідок непростої установки додаткових сенсорів (нині необхідний фізичний розрив з'єднання);

залежність продуктивності мережі при взаємодії з зовнішніми сегментами від продуктивності *IDS*;

мережевий інтерфейс, на якому виконується спостереження, може бути керуючим.

Всередині мережеві засоби мережевого захисту використовують як мережеву, так і хостову моделі виявлення МА. Даний факт дозволяє використовувати всі переваги таких моделей, а саме методики та алгоритми, що враховують характеристики МА, такі як події, зареєстровані в журналах:

конкретної операційної системи;

журналах додатків, що використовуються на хості;

міжмережевих екранів.

У цих засобах аналіз мережевого трафіку здійснюється безпосередньо в мережі, тобто аналізуються дані, взяті з технічних каналів зв'язку, з використанням середовища передачі даних і канал утворюючого обладнання обчислювальної мережі, шляхом застосування відповідних методик і алгоритмів мережевого аналізу даних.

До таких засобів відносяться більшість відомих і перерахованих на сьогодні програмних продуктів.

Засоби мережевого захисту між ЛОМ пропускають через себе весь мережевий трафік, що проходить між сегментами розподіленої обчислювальної мережі. При використанні таких засобів вузли ЛОМ не задіяні у виявленні атак і у разі виявлення мережевої деструктивної дії атаки, спрямовану на вузли ЛОМ, блокується на початковому етапі реалізації МА.

До таких засобів, наприклад, відносяться: мережеве рішення компанії *Ranch Networks* і Російська СВА *Intrusion Prevention – Proventia G* і *Proventia M*.

До відмінних властивостей таких засобів можна віднести:

захист від *dos*-атак;

ідентифікацію та авторизацію користувачів;

зміну стратегії захисту мережі залежно від її стану (*policy driven security-on-demand*);

захист мережі за індивідуальними адресами;

захист як вхідних, так і вихідних інформаційних потоків для кожної зони;

підтримку мережевої безпеки бездротової передачі даних (*wifi*) і передачі голосу через інтернет (*voip*);

зручне підключення до систем виявлення несанкціонованого доступу, а також програм вірусів і «черв'яків» (*IDS*).

Аналіз параметрів та характеристик захищеної ІС.

Під захищеною ІС розуміється система, в якій використовуються персональні комп'ютери (ПК), технічні канали зв'язку, які передбачають середовище передачі даних і канал утворюючого обладнання ЛОМ.

У таку ІС входять:

програмне забезпечення, що використовується під час роботи користувачів і виконання основних функцій по роботі з базами даних, клієнтськими додатками та ін.;

технічні засоби – вузли ЛОМ, комунікаційне і каналоутворююче обладнання та лінії зв'язку між ними, сукупність яких утворює фізичну топологію мережі;

програмні засоби, що забезпечують функціонування, а також фізичну та логічну взаємодію всіх технічних засобів, що входять в ІС, такі як системне ПЗ, спеціалізоване мережеве ПЗ.

Основною проблемою і обов'язковою умовою у створенні захищеної ІС є формалізація методу опису предметної області та оперування моделями, які адекватно описують архітектуру і функціонування об'єкта, що проєктується. Для опису платформи безпеки (ПБ) розподілених ІС використовують формалізм семантичних мереж фреймів:

В основі мережевих моделей лежить конструкція виду (3):

$$H = \{I, C_1, C_2, ..., C_n, \tilde{A}\} \quad (3)$$

де I – множина інформаційних одиниць;,

$C_i, C_2, ..., C_n$ – множина типів зв'язків між елементами;

Γ – відображення, що задає зв'язок з прийнятого набору між інформаційними одиницями.

З точки зору захищеності ІС розглядають графову модель системи захисту з повним перекриттям.

У цій моделі розглядається взаємодія «області загроз», «область, що захищається» (ресурсів АС) і «Системи захисту» (механізмів безпеки АС).

Так, маємо три множини:

$T = \{t_i\}$ – множина загроз безпеки;

$O = \{o_j\}$ – множина об'єктів (Ресурсів) захищеної системи;

$M = \{m_k\}$ – множина механізмів безпеки.

Елементи цих множин знаходяться між собою у певних відношеннях, власне і описують систему захисту.

Для опису системи захисту зазвичай використовується графова модель. Множина відношень загроза – об'єкт утворює дводольний граф $\{<T, O>\}$. Мета захисту полягає в тому, щоб перекрити всі можливі ребра в графі. Це досягається введенням третього набору M. У результаті виходить тридольний граф $\{<T, M, O>\}$. Розвиток цієї моделі припускає введення ще двох елементів:

V – набір вразливих місць, які визначаються підмножиною декартового добутку $T*O$: $vr = <t_i, o_j>$. Так, під вразливістю системи захисту будемо розуміти можливість здійснення загрози t відносно об'єкта o (на практиці під вразливістю системи захисту зазвичай розуміється не сама можливість здійснення загрози безпеки, а ті властивості системи, які сприяють успішному здійсненню загрози, або можуть бути використані зловмисником для здійснення загрози);

B – набір перешкод, що визначається декартовим добутком $V*M$: $b_i = <t_i, O_j, m_k>$, які являють собою шляхи здійснення загроз безпеці, перекриті засобами захисту.

Відповідно, при побудові систем захисту, що використовують виявлення МА, необхідно використовувати існуючі мережеві та хостові моделі, що містять сигнатурні та статистичні методи для повного перекриття підсистемами захисту M вдалого здійснення МА.

Загалом ІС повинна надавати такі види послуг:

встановлення зв'язку – реалізується засобами каналоутворюючого обладнання за допомогою каналів зв'язку;

передача даних – ЛОМ оснащена апаратурою та каналами передачі даних для забезпечення заданих швидкостей і надійності обробки даних.

Параметри, що захищаються ІС, повністю підходять під описані нижче.

Залежно від виду засобів, методів і алгоритмів керування, можна виділити ІС з централізованим і розподіленим управлінням. При цьому можуть виконуватися як жорсткі, так і гнучкі алгоритми управління ІС, що враховують численні фактори. Об'єднання мереж здійснюється або через загальний вузол, або шляхом створення спеціальних каналів, з'єднують вузли однієї системи з вузлами іншої. Якщо мережа може бути з'єднана з іншими, то вона називається відкритою, якщо ні, то – закритою.

За функціонально-цільовим і прикладним призначеннями ІС можна розділити на дві групи: загального користування та спеціального призначення.

ІС загального користування призначені для різних сфер застосування незалежно від конкретного змісту даних, що обробляються в ІС. Засоби, структура і функціональні можливості виявляються однаковими для багатьох випадків застосування і забезпечують широкий діапазон послуг.

ІС спеціального призначення призначені для вирішення завдань у певній предметній або відомчій областях.

Якісні характеристики ІС поділяються за такими показниками:

загальне число зв'язків;

тимчасові характеристики якості ІС;

середній час обслуговування;

надійність обслуговування;

достовірність передачі;

можливість доступу.

Характеристики засобів, що забезпечують обробку даних в ІС, охоплюють:

технічні засоби (сервера, робочі станції, комунікаційне обладнання, міжмережеві екрани) і лінії зв'язку між ними, сукупність яких утворює фізичну топологію АС (ЛОМ) та точки взаємодії (Стики) з іншими АС;

програмні засоби, що забезпечують функціонування, а також фізичну і логічну взаємодію (канали керування і передачі даних) всіх технічних засобів, що входять до АС (системне ПЗ, спеціалізоване мережеве ПЗ);

прикладне та сервісне програмне забезпечення, що розробляється окремо від загальносистемного ПЗ і виконує покладені на нього функції в рамках реалізації тієї чи іншої інформаційної технології (СУБД, офісні додатки, редактори, компілятори, *WEB*-сервера й ін.).

Мається на увазі, що компоненти ЛОМ розосереджені в просторі і зв'язок між ними фізично здійснюється за допомогою мережевих з'єднань, а програмно – за допомогою механізму повідомлень, заснованого на стеку протоколів *TCP/IP*. При цьому всі керуючі повідомлення і дані пересилаються між об'єктами ЛОМ, передаються мережевими з'єднаннями у вигляді пакетів обміну.

Характеристики захищеності ІС містять:

категорії оброблюваної в ІС інформації, вищий гриф секретності;

загальну структурну схему і склад ІС, в яку входять (перелік і склад устаткування, технічних і програмних засобів, користувачів, даних та їхніх зв'язків, особливості конфігурацій і архітектури);

тип ІС (одно- або багатокористувацька система, відкрита мережа, одно- або багаторівнева система);

обсяги основних інформаційних масивів і потоків;

швидкість обміну інформацією і продуктивність системи при рішенні функціональних завдань;

тривалість процедури відновлення працездатності після збоїв, наявність засобів підвищення надійності та живучості;

технічні характеристики каналів зв'язку (пропускна здатність, типи кабельних ліній, види зв'язку з віддаленими сегментами ІС і користувачами);

територіальне розташування компонентів ІС, їхні фізичні параметри;

наявність особливих умов експлуатації.

Класифікація атак на ІС із найбільш повних:

за характером впливу;

за метою впливу;

за умовою початку здійснення впливу;

за наявності зворотного зв'язку із об'єктом атаки;
за розташуванням атакуючого до об'єкта атаки;
за кількістю атакуючих;
за рівнем еталонної моделі *ISO/OSI*, на якому здійснюється вплив;
з причини появи помилки захисту, яка використовується;
за об'єктом атаки;
за способом впливу на об'єкт атаки;
за засобами атаки, що використовується;
за станом об'єкта атаки;
за силою впливу на область ураження.

Також атаки поділяються на категорії за методами і засобам їх проведення:
віддалене проникнення (*remote penetration*);
локальне проникнення (*local penetration*);
віддалена відмова в обслуговуванні (*remote denial of service*);
локальна відмова в обслуговуванні (*local denial of service*);
мережеві сканери (*network scanners*);
сканери вразливостей (*vulnerability scanners*);
зломщики паролів (*password crackers*);
аналізатори протоколів (*sniffers*).

Висновки. Основні проблемні питання:

складність об'єднання усіх принципів створення систем виявлення і протидії атакам до однієї системи;

зростання переліку загроз із розвитком технічної та програмної складової АС;

можливість виявлення лише деяких відомих видів атак;

відсутність нормативної законодавчої бази щодо відповідальності за реалізацію КА та вторгнень.

Перспективи подальших досліджень. Розглянуті у статті основні проблемні питання: стосовно складності об'єднання усіх принципів створення систем виявлення і протидії атакам до однієї системи; зростання переліку загроз із розвитком технічної та програмної складової АС; можливість виявлення лише деяких відомих видів атак; відсутність нормативної законодавчої бази щодо відповідальності за реалізацію КА та вторгнень, – потребують подальших досліджень переліку загроз та класифікації видів атак, розробки нормативної законодавчої бази та її наповнення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Куссуль Н. Н., Соколов А. М.. Адаптивное обнаружение аномалий в поведении пользователей компьютерных систем с помощью марковских цепей изменяющегося порядка // Кибернетика и вычислительная техника.

2. J. Allen et al. State of the practice of intrusion detection technologies. TR CMU/SEI-99-TR-028, Carnegie Mellon University, Software Engineering Institute, Pittsburgh, Jan. 2000.

3. D. Wagner and R. Dean. Intrusion detection via static analysis. In Proc. of the 2001 IEEE Symposium on Security and Privacy, pages 156–169, Los Alamitos, CA, May 14-16 2001.

4. Фленов М. Е. PHP глазами хакера. СПб.: БХВ-Петербург, 2005. 304 с.

5. Denning, D. 1986. An intrusion-detection model. In Proceeding of 1986 IEEE computer society symposium on research in security and privacy held in Oakland, California, April 7–9, 1986, by IEEE Computer Society, 118 – 31. Los Alamitos, CA: IEEE Computer Society Press.

6. Дэвид Г. Метод парных сравнений. М.: Статистика, 1978. 218 с.

7. Тоценко В. Г. Методы и системы поддержки принятия решений. Алгоритмический аспект. К.: Наукова думка, 2002. 381 с.

8. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Введ. 28.04.1999. К.: ДСТСЗИ СБ Украины, 1999.

9. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Введ. 28.04.1999. К.: ДСТСЗИ СБ Украины, 1999.

10. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Введ. 04.12.2000. К.: ДСТСЗИ СБ Украины, 2000.

11. Нелешенко В. С. Обзор методик обнаружения сетевых атак // Инфокоммуникационные технологии в науке и технике: материалы второй международной научно-технической конференции, часть II, 2006.

12. Чипига А. Ф., Пелешенко В. С. Обзор моделей систем обнаружения атак в ЛВС и выявление их недостатков // Инфокоммуникационные технологии в науке и технике: материалы второй международной научно-технической конференции, часть II, Ставрополь, 2006.

13. Чипига А. Ф., Пелешенко В. С. Формализация процедур обнаружения и предотвращения сетевых атак // Известия ТРТУ. Таганрог: Изд-во ТРТУ, 2006.

УДК 621.396

Руденко В. І. ORCID:0000-0003-3563-548X (ВІТІ ім. Героїв Крут)
Остапук О. І. ORCID:0000-0001-6557-9525 (ВІТІ ім. Героїв Крут)
Зінченко М. О. ORCID:0000-0002-1428-8231 (ВІТІ ім. Героїв Крут)
Яковчук О. В. ORCID:0000-0002-6312-5009 (ВІТІ ім. Героїв Крут)

ПОРЯДОК СТВОРЕННЯ ОБ'ЄКТІВ ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ МЕРЕЖ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

У цій статті розглядається електронна комунікаційна мережа, яка є складовою частиною та матеріально-технічною основою системи управління Збройними силами України. Проведений аналіз основних публікацій та досліджень в області створення об'єктів електронних комунікаційних мереж спеціального призначення показав, що на сьогодні не існує статей та матеріалів щодо порядку створення об'єктів електронних комунікаційних мереж. Враховуючи вказане, у статті обґрунтовуються та визначаються нормативні документи, на які необхідно спиратися командирам (начальникам) під час проведення проєктних та будівельних робіт щодо створення об'єктів електронних комунікаційних мереж. На ряду з цим формуються основні етапи створення військових об'єктів та визначаються алгоритми дій командирів (начальників). Вказується, що створення об'єктів електронних комунікаційних мереж спеціального призначення нерозривно пов'язано з проєктуванням та будівництвом цивільних об'єктів електронних комунікацій. Організація будівництва об'єктів Збройних сил України відбувається згідно з Положенням про організацію будівництва об'єктів у Міністерстві оборони та Збройних силах України, а саме будівництво здійснюється відповідно до законів України, підзаконних актів, державних будівельних норм, стандартів, правил та інших нормативно-правових актів, які регламентують діяльність у сфері будівництва. За результатами дослідження робиться висновок, що тільки суворе дотримання командирами (начальниками) нормативних документів Мінрегіону України в будівництві військових об'єктів забезпечить не тільки правильну організацію даних робіт, а й звітування за використані кошти.

Ключові слова: *електронні комунікації, електронна комунікаційна мережа, проєктування, будівництво, об'єкт будівництва, категорія складності, проєктна документація.*

V. Rudenko, M. Zinchenko, O. Yakovchuk, O. Ostapuk Procedure for creating objects of special purpose electronic communication networks.

This article examines the electronic communication network, which is an integral part and the material and technical basis of the management system of the Armed Forces of Ukraine. The analysis of the main publications and researches in the field of creation of objects of special purpose electronic communication networks showed that there are currently no articles and materials on the order of creation of objects of electronic communication networks. Taking into account the above, the article substantiates and defines normative documents that commanders (chiefs) need to rely on when carrying out design and construction work during the creation of electronic communication network facilities. Along with this, the main stages of the creation of military facilities are formed and the algorithms of actions of commanders (chiefs) are determined. It is indicated that the creation of objects of special purpose electronic communication networks is inextricably linked with the design and construction of civil objects of electronic communications. Organization of the construction of facilities of the Armed Forces of Ukraine takes place in accordance with the Regulation on the organization of construction of facilities in the Ministry of Defense and the Armed Forces of Ukraine, and the construction itself is carried out in accordance with the laws of Ukraine, by-laws, state building regulations, standards, rules and other legal regulations acts that regulate activities in the field of construction. Based on the results of the study, it is concluded that only strict compliance by the commanders (chiefs) of the normative documents of the Ministry of the Region of Ukraine in the construction of military facilities will ensure not only the correct organization of these works, but also accountability for the funds used.

Keywords: *electronic communications, electronic communication network, design, construction, construction object, complexity category, project documentation.*

Вступ. Досвід ведення війни з росією показав необхідність приділяти особливу увагу розвитку електронних комунікаційних мереж Збройних сил України (далі – ЕКМ ЗС України), які є основою управління військами. Дане пояснення випливає з того, що військові мережі не повною мірою задовольняють управління військами, потребують переобладнання, реконструкції, модернізації та будівництва мереж із впровадженням сучасних технологій.

Без технічного переоснащення ЕКМ ЗС України, розширення номенклатури послуг, що надаються, неможливо ефективно управляти військами.

Постановка задачі. ЕКМ – комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг [1].

За останній період активно розвиваються ЕКМ, впроваджуються перспективні апаратно-програмні засоби різного призначення (комутатори, маршрутизатори, мультиплексори і т. ін.) та проводиться модернізація споруд і технічних засобів ЕКМ ЗС України. Дуже часто трапляється, що командири з'єднань (частин, підрозділів) й інші посадові особи та керівники підприємств ЗС України та Міністерства оборони України (далі – МО України) (в подальшому – командири (начальники), які можуть виконувати функції замовника) під час створення об'єктів військових ЕКМ не можуть правильно організувати ці роботи та відзвітувати за використані кошти. Внаслідок чого правоохоронні органи України часто повідомляють про підозру розпорядникам коштів – командирам (начальникам) у заволодінні бюджетними коштами шляхом зловживання службовим становищем та службовому підробленні, що спричинило відповідно до Кримінального кодексу України тяжкі наслідки.

Метою статті є визначення законів України, підзаконних актів, державних будівельних норм, стандартів, правил та інших нормативно-правових актів, на які необхідно спиратися командирам (начальникам) під час проведення планувальних та підготовчих заходів, передпроєктних, проєктних та будівельних робіт щодо створення об'єктів ЕКМ ЗС України.

Виклад основного матеріалу дослідження

1. Аналіз основних нормативних документів, які регламентують створення об'єктів ЕКМ спеціального призначення

Основним нормативно-правовим актом, який визначає правові та організаційні основи державної політики України у сфері електронних комунікацій, в тому числі і в створенні об'єктів ЕКМ ЗС України, є Закон України від 16.12.2020 № 1089-IX «Про електронні комунікації».

1.1. Закон про електронні комунікації

Електронна комунікація (телекомунікація) – передавання та/або приймання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій.

Дія цього Закону поширюється на відносини у сфері електронних комунікацій щодо надання та отримання електронних комунікаційних послуг, постачання та доступу до ЕКМ.

Створення об'єктів ЕКМ ЗС України відбувається відповідно до Статті 25 цього Закону:

Розміщення на земельних ділянках об'єктів будівництва, що є частиною ЕКМ чи їхньої інфраструктури, повинно здійснюватися відповідно до Земельного кодексу України та Закону України «Про регулювання містобудівної діяльності».

Уздовж повітряних, підземних кабельних ліній та споруд ЕКМ встановлюються охоронні зони і просіки з дотриманням вимог Земельного та Лісового кодексів України.

Використання майна для розміщення технічних засобів електронних комунікацій та доступу до елементів інфраструктури об'єктів будівництва, що перебувають (не перебувають) у власності, здійснюється відповідно до Закону України «Про доступ до об'єктів будівництва, транспорту, електроенергетики з метою розвитку електронних комунікаційних мереж».

Встановлення (розміщення) технічних засобів електронних комунікацій, споруд ЕКМ на елементах інфраструктури об'єктів будівництва здійснюється на підставі **проєктної документації** [1, п. 7].

Другим нормативно-правовим актом, який визначає створення ЕКМ, є Закон України від 25.12.2015 № 922-VIII (зі змінами) «Про публічні закупівлі».

1.2. Закон про публічні закупівлі

Перед тим, як приступити до створення об'єктів ЕКМ ЗС України, необхідно визначитись, що це є: послуга, робота або товар. Нерідко командири (начальники) плутають послуги зв'язку, роботи та товари.

Даний Закон визначає правові та економічні засади здійснення закупівель товарів, робіт і послуг для забезпечення потреб держави (ЗС України). Цей Закон забезпечує: ефективне та прозоре здійснення закупівель; створення конкурентного середовища у сфері публічних закупівель; запобігання проявам корупції та адаптує законодавство України до Європейського Союзу.

Відповідно до цього нормативно-правового акту:

роботи – це розроблення проєктної документації на об'єкти будівництва, науково-проєктної документації на реставрацію пам'яток архітектури та містобудування, будівництво нових, розширення, реконструкція, капітальний ремонт та реставрація існуючих об'єктів і споруд виробничого та невиробничого призначення, роботи з нормування в будівництві, геологорозвідувальні роботи, технічне переоснащення діючих підприємств та супровідні роботам послуги, у тому числі геодезичні роботи, буріння, сейсмічні дослідження, аеро- і супутникова фотозйомка та інші послуги, що включаються до кошторисної вартості робіт, якщо вартість таких послуг не перевищує вартості самих робіт;

послуги – це будь-який предмет закупівлі, крім товарів і робіт, зокрема транспортні послуги, освоєння технологій, наукові дослідження, науково-дослідні або дослідно-конструкторські розробки, медичне та побутове обслуговування, найм (оренда), лізинг, а також фінансові та консультаційні послуги, поточний ремонт, поточний ремонт з розробленням проєктної документації;

товари – це продукція, об'єкти будь-якого виду та призначення, у тому числі сировина, вироби, устаткування, технології, предмети у твердому, рідкому і газоподібному стані, а також послуги, пов'язані з постачанням таких товарів, якщо вартість таких послуг не перевищує вартості самих товарів.

З огляду на ці визначення та Закон про електронні комунікації, можна зробити висновок, що створення (будівництво) об'єктів ЕКМ ЗС України відноситься до робіт. Тому дані роботи повинно регулювати на ряду із МО України та ЗС України і Міністерство розвитку громад та територій України (Мінрегіон).

Усі роботи зі створення об'єктів ЕКМ ЗС України повинні відбуватися відповідно до державних будівельних норм (ДБН), стандартів, правил та інших нормативно-правових актів даного міністерства.

Для того щоб створити об'єкт ЕКМ ЗС України (побудувати вузол електронних комунікацій, кабельну каналізацію, передавальний або приймальний радіоцентри; прокласти лінію зв'язку; модернізувати лінійно-апаратний цех; установити нове обладнання й т. ін.), необхідно розробити **проєктну документацію**. На основі затвердженої проєктної документації здійснюється будівництво об'єктів ЕКМ ЗС України.

Розроблення проєктної документації повинно відбуватися відповідно до затверджених Мінрегіоном України ДБН А.2.2-3:2014 «Склад та зміст проєктної документації на будівництво», які визначають вимоги до складу та змісту проєктної документації на будівництво об'єктів ЕКМ ЗС України.

1.3. Склад та зміст проєктної документації на будівництво

Проєктна документація на будівництво повинна відповідати положенням законодавства, вимогам містобудівної документації, будівельним нормам, стандартам та правилам.

На нових земельних ділянках будівництва інженерні вишукування повинні виконуватися відповідно до ДБН А.2.1-1, а при реконструкції та капітальному ремонті об'єктів – без уточнення раніше виконаних інженерних вишукувань та інструментального обстеження об'єктів.

Оформлення проєктної документації повинно здійснюватися згідно з нормативними документами комплексу А.2.4 «Система проєктної документації для будівництва» (Основні вимоги до проєктної та робочої документації ДСТУ Б А.2.4.-4:2009 – зі змінами).

Розроблення проєктної документації повинно відбуватися на підставі таких вихідних даних:

містобудівних умов і обмежень забудови земельної ділянки;

технічних умов;

завдання на проєктування;

інших вихідних даних.

Технічні умови щодо інженерного забезпечення об'єкта будівництва повинні передбачати виключно ті роботи і в тих обсягах, які необхідні для здійснення інженерного забезпечення об'єкта будівництва, що проєктується.

Клас наслідків (відповідальності) об'єктів ЕКМ ЗС України визначається відповідно до Державного стандарту України ДСТУ 8855:2019 «Будівлі та споруди. Визначення класу наслідків (відповідальності)».

Виходячи з класу наслідків (відповідальності), проєктування для об'єктів I, II, III, IV та V категорій складності здійснюються в одну, дві або три стадії.

Проєктна документація на будинки, будівлі, споруди, лінійні об'єкти інженерно-транспортної інфраструктури (об'єкти ЕКМ ЗС України), їх черги та/або пускові комплекси має бути розроблена з урахуванням будівельних норм та стандартів, чинних на час передачі її командиру (начальнику).

Проєктування може виконуватись за чергами будівництва, а також із виділенням пускових комплексів, якщо це передбачено завданням на проєктування. Визначення вартості проєктних робіт та експертизи проєктної документації на будівництво об'єктів ЕКМ відбувається відповідно до Кошторисних норм України «Настанова визначення вартості проєктних, науково-проєктних, вишукувальних робіт та експертизи проєктної документації на будівництво».

2. Аналіз основних керівних документів ЗС України, які регламентують створення об'єктів ЕКМ спеціального призначення

Основним керівним документом, який визначає порядок планування, проєктування, організації та фінансування будівництва об'єктів військових частин ЗС України, в тому числі будівництво (створення) об'єктів ЕКМ ЗС України, є Положення про організацію будівництва об'єктів у МО України та ЗС України (далі – Положення), затверджене Наказом МО України від 05.06.2019 № 284.

2.1. Загальні положення з організації будівництва в ЗС України

Будівництво об'єктів ЕКМ ЗС України здійснюється з метою створення належних умов їх функціонування відповідно до чинного законодавства.

Будівництво, реконструкція та капітальний ремонт об'єктів ЕКМ ЗС України (у тому числі, виконання передпроєктних, вишукувальних, проєктних, будівельних, монтажних та пусконалагоджувальних робіт) здійснюється відповідно до Плану будівництва, реконструкції та капітального ремонту об'єктів загальновійськового та спеціального призначення ЗС України за відповідною бюджетною програмою (підпрограмою) на відповідний рік (далі – План будівництва об'єктів ЗС України), який затверджується Міністром оборони України.

Замовником будівництва об'єктів ЕКМ ЗС України, які споруджуються за рахунок коштів державного бюджету та інших джерел, не заборонених законодавством, є МО України.

Виконання функцій замовника проєктування, будівництва об'єктів ЕКМ ЗС України покладаються на:

органи військового управління, територіальні управління капітального будівництва, квартирно-експлуатаційні управління командувань видів, родів, військ та сил ЗС України,

військові частини, військові навчальні заклади та інші суб'єкти господарювання на підставі довіреності МО України, або відповідно до своїх Положень (Статутів).

Виконавці функцій замовника (командири, начальники) під час будівництва об'єктів ЕКМ ЗС України можуть:

отримувати містобудівні умови та обмеження на будівництво;

забезпечувати об'єкти будівництва необхідною проєктною документацією;

отримувати дозвільні документи на виконання підготовчих та будівельних робіт;

проводити підготовку матеріалів для проведення закупівлі робіт із проєктування та будівництва, а також інших робіт і послуг, що включаються до загальної кошторисної вартості об'єктів ЕКМ ЗС України;

укладати договори на виконання робіт, виготовлення проєктної документації;

організовувати технічний та авторський нагляд у визначеному законодавством порядку;

контролювати виконання умов договорів, у тому числі щодо строків виконання робіт;

оформляти документи щодо прийняття в експлуатацію закінчених будівництвом об'єктів, у тому числі реєстрації декларації або отримання сертифікату в органах державного архітектурно-будівельного контролю.

2.2. Організація планування будівництва об'єктів ЕКМ ЗС України

У МО України проводиться:

середньострокове планування (на 3–5 років) шляхом розроблення Перспективного плану будівництва об'єктів ЗС України;

поточне планування (на один рік) шляхом розроблення та затвердження Плану будівництва об'єктів ЗС України на відповідний рік.

Перспективний план будівництва об'єктів ЗС України розробляється відповідальними за формування і виконання бюджетних програм (підпрограм) МО України та затверджується Міністром оборони України.

План будівництва об'єктів ЗС України на відповідний рік розробляється відповідальними за формування і виконання бюджетних програм (підпрограм) МО України на підставі затвердженого кошторису МО України. Після прийняття Державного бюджету України та затвердження Плану будівництва об'єктів ЗС України він доводиться до командирів (начальників). Командири (начальники) складають, затверджують та подають на погодження до відповідальних за формування і виконання бюджетних програм (підпрограм) МО України титули об'єктів будівництва, які фінансуються у відповідному році. Титули об'єктів складаються на будівництво, реконструкцію та капітальний ремонт об'єктів ЗС України за відповідною бюджетною програмою (підпрограмою) на відповідний рік.

2.3. Проєктування будівництва об'єктів ЕКМ ЗС України

Основним нормативним документом, який визначає вимоги до складу та змісту проєктної документації на будівництво об'єктів ЕКМ ЗС України, є ДБН А.2.2-3:2014 «Склад та зміст проєктної документації на будівництво».

Розроблення проєктної документації відбувається на підставі завдання на проєктування, в якому обґрунтовуються вимоги командирів (начальників) до планувальних, архітектурних, інженерних і технологічних рішень об'єкта будівництва, його основних параметрів та організації будівництва з урахуванням технічних умов та містобудівних умов і обмежень. Завдання на проєктування об'єкта ЕКМ ЗС України розробляється під керівництвом командира (начальника) з урахуванням класу наслідків (відповідальності) об'єкта будівництва, а також на підставі тактико-технічного завдання, яке готується військовими частинами, яким в подальшому ці об'єкти будуть надані в оперативне управління.

Клас наслідків (відповідальності) об'єктів ЕКМ ЗС України визначається відповідно до Державного стандарту України ДСТУ 8855:2019 «Будівлі та споруди. Визначення класу наслідків (відповідальності)».

Тендерний комітет (уповноважена особа/особи) під керівництвом командирів (начальників) проводять на електронному майданчику E-tender.UA (PROZORRO) відбір виконавців проєктних, вишукувальних робіт та/або будівництва, укладають договори, приймають виконані роботи у визначених законодавством порядку та строки.

Проєктування (роботи, які пов'язані зі створенням проєктної документації на будівництво) об'єктів ЕКМ ЗС України здійснюється проєктними організаціями (які мають на це право) на підставі договорів.

Договір (на проєктування та/або будівництво) укладається відповідно до Цивільного кодексу України, Господарського кодексу України, Загальних умов укладання та виконання договорів підряду в капітальному будівництві, затверджених постановою Кабінету Міністрів України від 01.08.2005 № 668 (зі змінами).

Договірна ціна вартості проєктних робіт розраховується відповідно до Кошторисних норм України «Настанова з визначення вартості проєктних, науково-проєктних, вишукувальних робіт та експертизи проєктної документації на будівництво», затверджених наказом Мінрегіону від 01.11.2021 № 281.

Командири (начальники) спільно з проєктною організацією надають на експертизу розроблену проєктну документацію до експертних організацій незалежно від форм власності, які відповідають визначеним Мінрегіоном критеріям.

Проведення експертизи здійснюється відповідно до ДСТУ 8907:2019 «Настанова щодо організації проведення експертизи проєктної документації на будівництво».

Після отримання експертного звіту щодо розгляду проєктної документації та її затвердження (схвалення) командири (начальники) можуть приступати до будівництва об'єктів ЕКМ ЗС України.

2.4. Будівництво об'єктів ЕКМ ЗС України

Будівництво (нове будівництво, реконструкція, капітальний ремонт та технічне переоснащення) об'єктів ЕКМ ЗС України здійснюється відповідно до законів України, підзаконних актів, державних будівельних норм, стандартів, правил та інших нормативно-правових актів, які регулюють діяльність у сфері будівництва.

Виконання підготовчих і будівельних робіт із будівництва на об'єктах ЕКМ ЗС України здійснюється з урахуванням вимог постанови Кабінету Міністрів України від 26.08.2015 № 747 «Порядок виконання підготовчих та будівельних робіт».

Тендерний комітет (уповноважена особа/особи) під керівництвом командирів (начальників) проводять на електронному майданчику E-tender.UA (PROZORRO) відбір виконавців будівництва у визначених законодавством порядку та строки.

Будівництво об'єктів ЕКМ ЗС України здійснюється на підставі договорів, які укладаються командирами (начальниками) відповідно до законодавства України в сфері державних закупівель.

Договірна ціна на будівництво об'єктів ЕКМ ЗС України базується на кошторисних нормах, нормативах, розрахункових показниках і поточних цінах трудових та матеріально-технічних ресурсів відповідно до Кошторисних норм України «Настанова з визначення вартості будівництва», затверджених наказом Мінрегіону від 01.12.2022 № 244.

Прийняття та оплата виконаних будівельних робіт командирами (начальниками) здійснюються:

при визначенні вартості виконаних обсягів робіт і проведенні взаєморозрахунків за виконані роботи – застосовуються первинні облікові документи «Акт приймання виконаних будівельних робіт» (форма № КБ-2в) і «Довідка про вартість виконаних будівельних робіт та витрати» (форма № КБ-3), які наведені у додатках 36 та 37 цієї Настанови;

при твердій договірній ціні за укрупненими показниками вартості – «Звіт про виконання робіт за контрактом на об'єкті будівництва за період (місяць/рік)», «Підсумковий звіт про

вартість виконаних робіт за контрактом на об'єкті будівництва за період» та «Акт здавання-приймання виконаних будівельних робіт», які наведено у додатках 38–40 цієї Настанови.

Прийняття і оплата виконаних проєктних та інших робіт здійснюється на підставі актів приймання-передачі виконаних робіт та накладних, передбачених законодавством та умовами укладених договорів.

Відповідальність за цільове використання бюджетних коштів несуть відповідальні за формування і виконання бюджетних програм (підпрограм) МО України, розпорядники бюджетних коштів та командири (начальники) згідно із законодавством.

Авторський та технічний нагляд за будівництвом об'єктів ЕКМ ЗС України здійснюється відповідно до постанови Кабінету Міністрів України від 11.07.2007 № 903 «Про авторський та технічний нагляд, під час будівництва об'єкта архітектури» (зі змінами) та Настанови щодо проведення авторського нагляду за будівництвом ДСТУ Н Б А.2.2-11:2014.

Після завершення робіт із будівництва об'єктів ЕКМ ЗС України прийняття в експлуатацію здійснюється згідно з порядком, затвердженим Кабінетом Міністрів України, а саме: Командирами (начальниками) складається Акт готовності об'єкта до експлуатації відповідно до «Порядку прийняття в експлуатацію закінчених будівництвом об'єктів» (зі змінами), затвердженого постановою Кабінету Міністрів України від 13.04.2011 № 461.

Один примірник Акта готовності об'єкта до експлуатації в місячний строк після завершення робіт надається до відповідальних за формування і виконання бюджетних програм (підпрограм) МО України.

Об'єкти ЕКМ ЗС України, які знаходяться на території військових частин (підрозділів), установ, організацій ЗС України, після завершення робіт на них командирами (начальниками) передаються на баланс до квартирно-експлуатаційних органів за територіальним принципом, у визначеному законодавством порядку. Якщо командир (начальник) є балансоутримувачем даного об'єкта, то він здійснює його подальше утримання та експлуатацію.

Фінансування будівництва об'єктів ЕКМ ЗС України здійснюється відповідно до Розділу 5 даного Положення.

3. Етапи створення об'єктів ЕКМ спеціального призначення

У цьому розділі ми розглянемо порядок дій командирів (начальників) при плануванні, проєктуванні і будівництві об'єктів ЕКМ ЗС України. Тим, хто не знайомий із будівництвом досить близько, може здатися, що нічого складного тут немає: вибрав ділянку (трасу прокладання лінії зв'язку), пригнав техніку і почав будівництво. Насправді все далеко не так, і від моменту прийняття рішення про будівництво до початку будівництва об'єкта може пройти не один місяць підготовчих робіт. Ми спробуємо детально розібратися, з чого починається будівництво, які документи необхідно підготувати та як їх правильно оформити.

Порядок створення об'єктів ЕКМ ЗС України – це складний і багатоетапний процес, який містить кілька етапів – від видання наказу про початок реалізації проєкту, будівництво об'єкта і прийом його в експлуатацію. Командири (начальники) відповідають за будівництво об'єктів, ведуть контроль за всіма етапами будівництва самостійно та/або можуть довірити підрядній організації, яка буде контролювати якість виконання робіт субпідрядників.

Основні роботи можна розділити на три етапи.

1-й етап. Передпроєктні роботи – роботи, які можуть виконуватися до початку процесу проєктування для визначення принципових об'ємно-просторових та містобудівних рішень [4].

2-й етап. Проєктування – роботи, які пов'язані зі створенням проєктної документації на будівництво [4]. Дані роботи повинні складатися з затверджених текстових та графічних матеріалів, якими визначаються містобудівні, об'ємно-планувальні, архітектурні, конструктивні, технічні, технологічні рішення, а також із кошторисів об'єктів будівництва.

Для розроблення проєктної документації необхідно:

заключити договір на виготовлення проєктної документації об'єкта будівництва з проєктною організацією, яка повинна мати в своєму складі спеціалістів із кваліфікаційними

сертифікатами (інженера-проєктувальника, розробника кошторисної документації, спеціалістів з оцінки впливу на довкілля, з проведення геодезичних робіт та інших). До договору додаються затверджені: завдання на проєктування; протокол узгодження договірної ціни; календарний план робіт; кошториси та інші документи. Склад, обсяг та зміст проєктної документації розробляється відповідно до будівельних норм та стандартів, чинних на дату передання її замовнику. Експертиза проєктної документації проводиться у випадках, передбачених законодавством. Вартість проєктних, науково-проєктних, вишукувальних робіт та експертизи проєктної документації на будівництво визначається відповідно до Кошторисних норм України «Настанови з визначення вартості проєктних, науково-проєктних, вишукувальних робіт та експертизи проєктної документації на будівництво», затверджених Наказом Мінрегіону від 01.11.2021 № 281. Проєктування закінчується прийомом командирами (начальниками) робіт з підписанням актів здачі-приймання виконаних проєктних, науково-проєктних, вишукувальних та додаткових робіт.

3-й етап. Будівництво – нове будівництво, реконструкція, капітальний ремонт та технічне переоснащення об’єктів будівництва [4].

Вибір будівельної організації, яка має ліцензію на будівництво, та укладання договору на виконання будівельно-монтажних робіт. Технічний та авторський нагляди за ходом будівництва, відповідність проєктній документації. Пусконалагоджувальні роботи. Введення об’єкта будівництва в експлуатацію – завершується оформленням Акта здавання-приймання виконаних будівельних робіт.

Нижче наводиться приблизний порядок дій, на який необхідно спиратися командирам (начальникам) у період від рішення про будівництво об’єктів ЕКМ ЗС України до введення їх в експлуатацію.

Порядок дій командирів (начальників) зі створення об’єктів ЕКМ ЗС України

№ з/п	Порядок дій	Примітка
	1-й етап. Передпроєктні роботи	
	1.1. Збір матеріалів для проєктування, вивчається об’єкт проєктування, формуються вимоги. 1.2. Розробляються попередні концептуальні архітектурні пропозиції та пропозиції щодо розміщення об’єкта будівництва на земельних ділянках (обґрунтовуються місця розташування, необхідна територія та умови будівництва). 1.3. Опрацьовуються технологічні та інженерні характеристики об’єкта. 1.4. Складаються завдання на інженерні вишукування. 1.5. Обмірюються та обстежуються об’єкти ЕКМ, які підлягають реконструкції, капітальному ремонту або технічному переоснащенню. 1.6. Розробляються вихідні дані (містобудівні умови та обмеження забудови земельної ділянки, технічні умови, проєкт завдання на проєктування). 1.7. Інші види робіт, які необхідні для початку процесу проєктування. 1.8. Затверджується передпроєктна документація і ухвалюється рішення на реалізацію проєкту. 1.9. Надається пропозиція на включення об’єкта проєктування в план будівництва об’єктів ЗС України на відповідний рік	

№ з/п	Порядок дій	Примітка
	2-й етап. Проєктування	
	2.1. Затвердження об’єкта проєктування в Плані будівництва об’єктів ЗС України на відповідний рік. 2.2. Видання наказу про початок реалізації проєкту і призначення відповідальних. 2.3. Розробка та затвердження вихідних даних (містобудівних умов та обмежень забудови земельної ділянки, технічних умов, завдання на проєктування). 2.4. Підготовка та надання до місцевих органів виконавчої влади документів, необхідних для отримання дозвільної документації на проєктування та будівництво об’єкта ЕКМ (при законодавчій необхідності). 2.5. Вибір проєктної (проєктної та будівельної) організації з укладанням договору на виконання проєктних робіт. 2.6. Експертиза проєктної документації (при законодавчій необхідності). 2.7. Затвердження проєктної документації з підписанням акту здачі-приймання виконаних проєктних, науково-проєктних, вишукувальних та додаткових робіт	Переговори, торги (залежно від вартості будівництва)
	3-й етап. Будівництво	
	3.1. Вибір будівельної організації та укладання договору на виконання будівельно-монтажних робіт. 3.2. Укладання договору на технічний та авторський нагляди (при законодавчій необхідності) за ходом будівництва, відповідність проєктній документації. 3.3. Будівництво та організація пусконалагоджувальних робіт. 3.4. Введення об’єкта будівництва в експлуатацію. Оформлення та затвердження акта здавання-приймання виконаних будівельних робіт	Переговори, торги (залежно від вартості будівництва)

Висновки. Проведений аналіз основних нормативних документів, які регламентують створення об’єктів ЕКМ ЗС України, показав, що будівництво – це складний і багатоетапний процес, який складається з передпроєктних, проєктних та будівельних робіт. Основним керівним документом, який визначає порядок планування, проєктування, організації та фінансування будівництва об’єктів військових частин ЗС України, є Положення про організацію будівництва об’єктів у МО України та ЗС України. Відповідальною особою за організацію будівництва та правильність використання коштів виступає виконавець функцій замовника – командир (начальник). Будівництво військових об’єктів відбувається відповідно до ДБН, затверджених Мінрегіоном України. Основними нормативними документами, які регламентують дане будівництво, є ДБН А.2.2-3:2014, Склад та зміст проєктної документації на будівництво та настанов з визначення вартості проєктних, науково-проєктних, вишукувальних робіт, експертизи проєктної документації та будівництва. Якщо командири (начальники) будуть правильно організовувати будівництво об’єктів ЕКМ ЗС України та своєчасно звітувати за використання коштів із суворим дотриманням нормативних документів, ніякі правоохоронні органи не зможуть пред’явити претензії до організаторів даних робіт.

Подальші напрямки передбачають проведення обговорення і вивчення нормативних документів з обліку матеріальних засобів та будівництва об’єктів військових ЕКМ з командирами (начальниками), відповідальними особами за правильну організацію даних робіт й звітування за використані кошти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX // Верховна Рада України: офіційний портал. URL: https://zakon.rada.gov.ua/laws/show/1089-IX#Text.

2. Про публічні закупівлі: Закон України від 25.12.2015 № 922-VIII (зі змінами) // Верховна Рада України: офіційний портал. URL: https://zakon.rada.gov.ua/laws/show/922-19#Text.

3. Про оборонні закупівлі: Закон України від 17.07.2020 № 808-IX (зі змінами) // Верховна Рада України: офіційний портал. URL: https://zakon.rada.gov.ua/laws/show/808-20#Text.

4. ДБН А.2.2-3:2014. Склад та зміст проєктної документації на будівництво.

5. Положення про організацію будівництва об’єктів у Міністерстві оборони України та Збройних Силах України: затв. наказом Міністерства оборони України від 05.06.2019 № 284.

6. Порядок визначення предмета закупівлі: наказ Мінекономрозвитку від 15.04.2020 № 708.

7. ДСТУ БА.2.4.-4:2009. Основні вимоги до проєктної та робочої документації (зі змінами).

8. ДСТУ 8855:2019. Будівлі та споруди. Визначення класу наслідків (відповідальності).

9. Кошторисні норми України «Настанова з визначення вартості проєктних, науково-проєктних, вишукувальних робіт та експертизи проєктної документації на будівництво»: затв. наказом Мінрегіону від 01.11.2021 № 281.

10. Кошторисні норми України «Настанова з визначення вартості будівництва»: затв. наказом Мінрегіону від 01.12.2022 № 244.

УДК 159.9.07; 377.3

д-р філос. наук, проф. Чорний В. С. (ВІТІ ім. Героїв Крут)
Османов Р. Н. (ВІТІ ім. Героїв Крут)
Сердюк П. Є. (ВІТІ ім. Героїв Крут)

ОСОБЛИВОСТІ ПСИХОЛОГІЧНОГО ЗАБЕЗПЕЧЕННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

У статті розглядаються особливості психологічного забезпечення в Збройних силах України. Обґрунтовується актуальність заявленої проблеми, пов'язаної з російсько-українською війною. Розкриваються особливості сучасних бойових дій під, час яких психологічна стійкість та бойова активність особового складу є найважливішими складовими, які забезпечують збереження бойової ефективності військ (сил) і досягнення перемоги у сучасному бою. З урахуванням досвіду провідних країн-членів НАТО визначаються напрями підтримання психологічної стійкості військовослужбовців в умовах російсько-української війни. Проведений аналіз психологічної стійкості у межах визначеної мети обумовили його спрямованість на вивчення психологічної стійкості військовослужбовців до екстремальних ситуацій у контексті пошуку ефективних методів її забезпечення.

Ключові слова: *психологічне забезпечення, психологічна стійкість; бойові дії; екстремальна ситуація; емоційне напруження; психологічні стани.*

V. Chornyi, R. Osmanov, P. Serduk Features of psychological support in the armed forces of Ukraine during the russian-Ukrainian war.

The article examines the peculiarities of psychological support in the Armed Forces of Ukraine. The relevance of the stated problem related to the Russian-Ukrainian war is substantiated. The features of modern combat operations are revealed, during which the psychological stability and combat activity of personnel are the most important components that ensure the preservation of the combat effectiveness of troops (forces) and the achievement of victory in modern combat. Taking into account the experience of the leading NATO member countries, directions are determined to support the psychological stability of military personnel in the conditions of the russian-Ukrainian war. The analysis of psychological resilience within the framework of the goal determined its focus on studying the psychological resilience of servicemen to extreme situations in the context of searching for effective methods to ensure it.

Keywords: *psychological support, psychological stability; fighting; extreme situation; emotional stress; psychological conditions.*

Постановка проблеми. Сучасна російсько-українка війна є якісно новим підходом до ведення збройної боротьби, ключовими моментами якого є застосування новітніх розробок озброєння та військової техніки, зміна тактики, оперативного мистецтва і стратегії, жорстке інформаційно-психологічне протиборство. За таких умов значно зростає важливість психологічного забезпечення як одного зі складових морально-психологічного забезпечення Збройних сил України.

За функціональним призначенням психологічне забезпечення – це цілеспрямована діяльність органів військового управління, командувачів, командирів (начальників), посадових осіб структур морально-психологічного забезпечення з метою психологічного відбору, формування, підтримання і відновлення в особового складу військових частин (підрозділів) психологічної готовності до виконання завдань за призначенням, психологічної стійкості до негативних психологічних чинників за будь-яких умов обстановки, зниження психогенних втрат та збереження психічного здоров'я військовослужбовців.

Нові завдання військових частин (підрозділів) Збройних сил України, пов'язані з триваючою російською агресією, передбачають підвищення ефективності усієї системи їхнього морально-психологічного забезпечення загалом і психологічного забезпечення зокрема. Усе це робить актуальною та практично значущою діяльність командирів (начальників), штабів, офіцерів структур морально-психологічного забезпечення щодо

психологічного забезпечення бойових дій – подолання особовим складом негативного впливу бойових стрес-факторів.

Сучасна російсько-українська війна засвідчила, що рівень підготовленості особового складу окремих військових частин (підрозділів) Збройних сил України до виконання бойових завдань, особливо в «нестандартних» умовах, не завжди відповідають сучасним вимогам [1].

Цілком очевидно, що вдосконалення професійної підготовки українських військовослужбовців необхідно розглядати разом з психологічними проблемами збереження ефективності їхньої військової діяльності та бойової активності.

При цьому пріоритетної актуальності набувають дослідження шляхів та способів підтримання високої психологічної стійкості та бойової активності особового складу під час ведення бойових дій, що є найголовнішою особливістю психологічного забезпечення в Збройних силах України на сучасному етапі російсько-української війни.

Аналіз останніх досліджень і публікацій. Сучасна російсько-українська війна актуалізувала питання глибокого переосмислення існуючих методик визначення бойових можливостей підрозділів військ (сил), засвідчила явища неповного врахування впливу психологічної стійкості на загальні показники бойових можливостей, що перешкоджає якісному виконанню бойових завдань. Зважаючи на вищезазначене, теоретичне підґрунтя нашого дослідження складають праці:

В. Стасюка, В. Ягупова та групи науковців, які виокремили залежність боєздатності особового складу від рівня сформованості мотивації та психологічної стійкості;

Г. Давидова, М. Бочарова, О. Блінова, О. Кокуна, В. Клименка, М. Варія, Ю. Московчука та ін., які обґрунтували, що врахування психологічної стійкості військ у бойових умовах можливе за допомогою методик контролю морально-психологічного стану, психологічної стійкості особового складу та прогнозування бойових психогенних втрат [2];

Г. Горелова, В. Невмержицького, О. Охріменка та Ю. Ярошок, які розглядають теоретичні і практичні засоби адаптації військовослужбовців до екстремальних умов несення військової служби. Проблеми адаптації деякою мірою також розглядали у працях такі науковці, як Н. Агаєв, Ю. Александровський, Ф. Березін, В. Бодров, С. Василенко, Ю. Ільченко, О. Кокун, М. Корольчук [6], В. Стасюк [3], О. Хайрулін, В. Чорний [4] та ін.;

І. Аршави, М. Бочарова, О. Донця, К. Кіма, В. Клочкова, С. Лисюка, Д. Шміголя, які розглядають психологічну стійкість особистості в екстремальних умовах;

А. Сірого, О. Кальчука та ін., які досліджують мотивацію особистості до діяльності в екстремальних умовах;

В. Кравченко, М. Зівзаха, С. Миронця, В. Садкового, О. Тімченко, які аналізують негативні стани особистості після впливу екстремальної ситуації [5];

С. Кобейс, С. Мадді, О. Таубман, В. Флоріан та ін. аналізують поняття «психологічна стійкість» в комплексі властивостей особистості, таких як опірність, урівноваженість, життєстійкість, стабільність тощо. Водночас С. Мадді розробив модель життєстійкості, що розглядає її як важливий людський ресурс з метою підтримання фізичного, психічного та соціального здоров'я, тому дослідник пов'язує «життєстійкість» із «переконаннями людини, що дозволяють їй залишатися активною і готовою долати негативні наслідки стресу» [6, с. 178];

А. Маслоу, Ф. Перлс, К. Роджерс, В. Франкл, Е. Фромм розглядають психологічне здоров'я у контексті формування психологічної стійкості особистості. Зокрема А. Маслоу основною ознакою психологічного здоров'я вважав прагнення індивіда розвивати свій потенціал через самоактуалізацію, реальні професійні та життєві досягнення, прагнення слідувати гуманістичним цінностям. На його думку, психологічно здорові люди характеризуються такими якостями, як автономія, спонтанність, чутливість до прекрасного, почуття гумору, творчість, здатність сприймати інших і себе [7, с. 96].

Під час підготовки матеріалу також були розглянуті основні погляди на визначення стійкості до стресу в інтерпретації В. Мільмана, В. Норакідзе, R. Cattell, J. Guilford, П. Фрес та

ін., а також напрями, які досліджують стійкість до стресу (традиційно-аналітичний, системно-регулятивний, системно-структурний); основні групи умов, що впливають на рівень психологічної стійкості.

Метою статті є розгляд особливостей психологічного забезпечення в Збройних силах України, визначення напрямів підтримання психологічної стійкості військовослужбовців в умовах російсько-української війни.

Викладення основного матеріалу. Ефективне виконання бойових завдань з мінімальними втратами – один з головних пріоритетів військ (сил). Сучасна бойова діяльність пов'язана з великими фізичними та психічними навантаженнями, які дестабілізують психіку військовослужбовців, знижують її ефективність, що негативно позначається на результатах виконання завдань за призначенням загалом.

Триваюча російсько-українська війна потребує високої підготовки та професіоналізму військовослужбовців, висуває більш високі вимоги до формування стійкості складних навичок, умінь та інших психічних утворень, їхнього підтримання тривалий час і за різних умов. Зважаючи на це виникає актуальна проблема аналізу та врахування різноманітних чинників, які впливають на психологічну стійкість особового складу під час бойових дій.

У бойовій обстановці психіка військовослужбовця зазнає безліч різноманітних впливів. Одні з них сприяють мобілізації та концентрації фізичних та духовних можливостей людини, підвищенню бойової активності, хоробрості, самовідданості. Інші, навпаки, дезорганізують бойову діяльність військовослужбовців, блокують доступ до наявних резервів організму, дестабілізують роботу нервової системи та психіки загалом. Треті не мають помітного впливу на бойову поведінку.

Наявна статистика та наукові дослідження стану цієї проблеми переконливо доводять необхідність правильного формування та підвищення бойової активності та психологічної стійкості військовослужбовців під час виконання завдань за призначенням. Так, зокрема, у період Першої світової війни психогенні втрати Збройних сил США склали 100 тис. осіб, у період Другої світової війни – 1 млн осіб. Під час війни у Кореї безповоротні психогенні втрати американців склали 4 особи, а у В'єтнамі – 7 осіб на кожну тисячу військовослужбовців. У період війни Ізраїлю проти Лівану 9 % ізраїльських солдатів і офіцерів були виведені із ладу через низьку психологічну стійкість та втрату бойової активності. За оцінками американських психологів зі складу військових частини, які перенесли ядерний вибух, лише 12–15 % військовослужбовців зберігає здатність виконувати завдання за призначенням, 75 % – тимчасово, а 10–15 % – на тривалий час втрачають боєздатність через розлади нервової системи [8, с. 47].

У Кувейтському конфлікті загальні психогенні втрати іракських військовослужбовців після масованих бойових ударів американської авіації протягом перших трьох діб склали: у регулярній армії – 45 %, серед ополченців-непрофесіоналів – 68–70 % [8, с. 47].

Останнім часом американське командування надає великого значення проблемам вироблення у військовослужбовців психологічної стійкості та бойової активності, розширення психологічних та психофізіологічних можливостей організму. Психологи США прогнозують, що у сучасній війні в Європі до 50 % усіх втрат можуть становити психогенні.

Вважається, що при достатньо високій психологічній стійкості військовослужбовців і оволодінні ними прийомами та методами психічної саморегуляції, більше половини уражених можуть повернутися до виконання своїх обов'язків через 1–3 доби [8, с.64].

Поряд із вищезазначеним, на сьогодні дедалі очевиднішим є той факт, що успішне досягнення мети професійної діяльності залежить не лише від особливостей та специфіки самої діяльності, навченості військовослужбовця, а і його характерологічних особливостей та особистісних якостей.

Більшість дослідників вважають окремі психофізіологічні та психологічні якості особистості умовою забезпечення надійності професійної діяльності, провідне місце у якій

посідає психологічна стійкість військовослужбовців. Наразі вважається, що психологічною стійкістю військовослужбовця під час військової діяльності є професійна якісна характеристика його особистості, обумовлена системою взаємопов'язаних особистісних якостей, професійно-діяльнісних та соціально-психологічних чинників.

Підтримання психологічної стійкості та бойової активності особового складу під час бойових дій забезпечується психологічно обґрунтованою організацією професійної підготовки та практичної діяльності, створенням сприятливих соціально-психологічних умов та використанням спеціальних методів психологічної регуляції.

Серед напрямів підтримання та підвищення психологічної стійкості і бойової активності військовослужбовців виділяють такі:

професійно-діяльнісний;

соціально-психологічний;

індивідуально-психологічний.

До професійно-діяльнісного напряму слід віднести такі:

знання та грамотна експлуатація озброєння та військової техніки;

формування та підтримання навичок ведення бою за різних умов;

професійно-психологічний відбір та розподіл військовослужбовців за військовими професіями з урахуванням їхніх характерологічних особливостей та особистих якостей;

облік, контроль і дозування психічного навантаження на кожного військовослужбовця відповідно до особливостей його військової професії та особистих якостей;

об'єктивна оцінка безпосередніми командирами (начальниками) результатів бойової діяльності кожного військовослужбовця та підрозділу загалом;

відпрацювання злагодженості бойової діяльності у розрахунках, екіпажах та підрозділах;

навчання військовослужбовців адекватній самооцінці результатів своєї діяльності;

проведення військово-спеціальних тренувань, які імітують умови, наближені до бойових;

індивідуальне та у складі розрахунку, екіпажу відпрацювання варіантів ведення бою з використанням тренажної апаратури;

підтримання високого рівня фізичної натренованості та витривалості;

запобігання щодо спрощень та перестраховки під час підготовки та ведення бойових дій.

До соціально-психологічного напряму можна віднести такі:

постійне і повне інформування особового складу військових частин (підрозділів) про умови та особливості майбутніх бойових дій;

формування та згуртування військових розрахунків, екіпажів та підрозділів;

правильний підбір, розстановка та комплектування розрахунків, екіпажів та відділень із урахуванням індивідуально-психологічних особливостей військовослужбовців;

розбір та аналіз причин загибелі військовослужбовців як один із засобів вироблення психологічного налаштування на бойові дії та усунення благодушності, самозаспокоєності, недбалості тощо;

забезпечення психологічної та функціональної сумісності розрахунків, екіпажів та відділень;

підтримання ситуативно-необхідного стилю керівництва розрахунком, екіпажем та відділенням з боку його командира;

підвищення культури взаємодій у підрозділах;

профілактика негативних соціально-психологічних явищ та процесів у підрозділах;

створення та підтримання необхідних товариських, професійних та ділових взаємин у підрозділах.

До індивідуально-психологічного напряму належать такі:

знання особистісних якостей кожного військовослужбовця;

виховання у військовослужбовців таких якостей, як почуття особистої відповідальності та дисциплінованості, хоробрості та рішучості; холоднокровності та розумної ініціативи тощо;

конкретна професійна, спеціальна та психологічна підготовка до кожного бою;

постійне підтримання досягнутого рівня військово-професійної натренованості;

запобігання тривалим перервам у бойовій діяльності;

планомірне введення військовослужбовців-новачків до бойової діяльності з поступовим збільшенням складності бойових завдань;

збереження психічного та фізичного здоров'я військовослужбовців шляхом використання методів психічної саморегуляції та корекції психічних станів.

Надзвичайно великий та повчальний досвід щодо підтримання психологічної стійкості та бойової активності військовослужбовців накопичений у провідних країнах НАТО. До зазначеної проблеми західні військові фахівці підходять комплексно. Існуючі наукові підходи до розуміння психологічної стійкості військовослужбовців розглядаються у сукупності з цілісними особистісними характеристиками, окремими особистісними якостями, констеляціями різних особистісних чинників, стилем поведінки тощо. Внаслідок цього психологічна стійкість аналізується у системі, заданій такими координатами:

вимоги подій;

стрес та копінг;

індивідуальні чинники;

організаційні чинники;

результат.

Це дозволяє дослідникам розглядати психологічну стійкість як багатовимірний конструкт, що містить безліч характеристик, які відображають здатність військовослужбовця або малої військової соціальної групи відновлювати свій стан чи адаптаційний процес, що дозволяє знижувати напругу бойової обстановки та хронічних стресів. Тобто психологічна стійкість – це не здатність зберігати незмінність своїх кондицій, а здатність «пружинити», «відскакувати», «пристосовуватися». Психологічна стійкість військовослужбовця, на думку західних вчених, проявляється при наявності у нього:

а) когнітивних ресурсів, що дозволяють ефективно вирішувати проблеми;

б) емоційних умінь протистояти стресові;

в) соціальних та сімейних ресурсів, які можуть бути залучені у потрібний час;

г) здатності знаходити мету та сенс своєї служби;

д) фізичної стійкості до тривалих труднощів [9].

На сьогодні, в провідних країнах НАТО (принаймні США, Великій Британії та Канаді) склалася ефективна система технологій формування психологічної стійкості військовослужбовців, яка включає:

Stress Management Training (тренінг управління стресом, тренінг щеплення стресу, медитації уваги тощо);

Preparatory Education – попереднє навчання (програма формування бойової свідомості *«Battlemind»*, надання військовослужбовцям необхідної інформації щодо психологічних явищ сучасного бою);

Stress-Related Cognitive Appraisals – формування ефективних копінг-стратегій;

Rolemodeling – використання поведінкових зразків для наслідування, досвіду бувалих військовослужбовців;

Exposure/Mission Rehearsal Exercises – тренування військовослужбовців у виконанні завдань в обстановці, максимально наближеної до бойової, зокрема з використанням технології віртуальної реальності;

Exposureto Internal Stimuli – тренування апарату стресового реагування.

У бойовій обстановці підтриманню психологічної стійкості військовослужбовців сприяють командири та фахівці з психічного здоров'я, які перебувають у таких пропорціях щодо військовослужбовців: у Британії – 1:2500–4000, США – 1:700, Канаді – 1:500–60.

До збереження психологічної стійкості включається психологічний актив – спеціально підготовлені військовослужбовці. У Британській армії, наприклад, діє *Trauma Risk Management program* – програма використання парамедичного персоналу (активу) на користь психологічної підтримки товаришів по службі.

По завершенні бойових дій учасники включаються до *Third-Location Decompression Program* – програми «декомпресії», тобто програми поступового (від 36 годин у британській армії, до п'яти діб у канадській) психологічного повернення учасників бойових дій до мирних умов життєдіяльності. 95 % ветеранів вважають цю програму необхідною та ефективною.

Водночас у США на сьогодні діє ексклюзивна і достатньо ефективна програма формування всебічної готовності військовослужбовців – *Comprehensive Soldier Fitness (CSF).* На стратегічному рівні ця програма відповідає на запитання: «Як зробити програму психологічної підготовки військовослужбовців збройних сил такою ж важливою, як і їхня фізична підготовка?».

На оперативному рівні вона показує, як командирам (начальникам) тренувати своїх підлеглих у військових частинах (підрозділах).

На тактичному рівні вона спрямована на навчання військовослужбовців способам подолання труднощів.

Програма формування всебічної готовності військовослужбовців CSF складається з чотирьох компонентів:

Global Assessment Tool (GAT) – програма оцінки всебічної готовності військовослужбовця (опитувальник, який налічує 105 запитань), що дозволяє спланувати подальший його розвиток;

Comprehensive Resilience Modules – 24 різних онлайн-модулі, що складають серцевину психологічної підготовки військовослужбовця, які відповідають рівню вихідної готовності, займаній посаді та досвіду;

Master Resilience Trainer Course (MRTs) – 10-денний курс підготовки сержантів як ведучих тренінгів;

Institutional Training – елементи тренінгу, вбудовані до усіх видів професійної підготовки та підвищення кваліфікації військовослужбовця [8, с. 124–136].

Як вважає більшість дослідників, зазначена програма формування всебічної готовності військовослужбовців Збройних сил США є ефективною і спроможною, при раціональних адаптації та використанні, посилити боєздатність збройних сил будь-якої держави. При цьому варто відзначити, що окремі її елементи вже імплементовані до практики діяльності Збройних сил України загалом і структур морально-психологічного забезпечення дій військ (сил) зокрема [9].

Висновки. Як свідчить бойовий досвід сучасної російсько-української війни, психотравмуюча ситуація, тривала фізична та психічна напруга змінюють особистісну сферу військовослужбовців, що порушує роботу регуляторних механізмів психіки, призводить до зниження психічної стійкості та наростання психічної нестійкості, створюють підґрунтя для психічних порушень та формування девіантної поведінки.

Зважаючи на це найголовнішою особливістю психологічного забезпечення в Збройних силах України на сучасному етапі є підтримання психологічної стійкості та бойової активності особового складу під час бойових дій. Доведено, що це забезпечується психологічно обґрунтованою організацією психологічної підготовки та практичної діяльності, створенням сприятливих соціально-психологічних умов та використанням спеціальних методів психологічної регуляції.

Відтак, діяльність командирів (начальників) штабів, офіцерів структур морально-психологічного забезпечення необхідно спрямувати на психологічне забезпечення бойових дій – подолання особовим складом негативного впливу бойових стрес-факторів, розвиток у підлеглих адаптаційних навичок, навичок асертивності та стресостійкості, вироблення

конструктивних механізмів адекватної поведінки, опрацювання психотравмуючих ситуацій психофізіологічними і психотерапевтичними методами, оскільки зазначена робота є невід'ємною і обов'язковою частиною підтримання психічного здоров'я і психологічного супроводу військовослужбовців, які беруть участь у бойових діях.

Водночас соціально-психологічну профілактичну роботу та психолого-педагогічні заходи впливу необхідно спрямовувати на зміцнення та стабілізацію психологічної стійкості військовослужбовців загалом, яка є свого роду «щепленням» проти різних форм девіантної поведінки тощо.

За межами даної роботи залишилося коло питань, що очікують свого вирішення, а саме дослідження проблеми соціально-психологічного супроводу військової служби засобами психологічних тренінгових технологій, які становлять сукупність ефективних навчально-розвивальних інтерактивних прийомів та методів. Розроблення циклу лекцій для командного складу Збройних сил України з основ екстреної психологічної допомоги підлеглим та особистісної психогігієни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бойко О. Контроль бойового стресу військовими лідерами // ГО "Український центр військового лідерства". 11 травня 2022 р. URL: https://enigma.ua/articles/kontrolb-boyovogo-stresu-viysbkovimi-liderami (дата звернення: 14.08.2023).

2. Бочаров М. М. Оцінка рівня психологічної стійкості особового складу в управлінні підрозділами військ (сил) // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2016. № 1. С. 88–92.

3. Стасюк В. В. Психологічне забезпечення діяльності військ (сил): підруч. К.: НУОУ, 2014. 504 с.

4. Vitalii Chornyi, Sergii Boltivets, Mykola Korolchuk, Valentyna Korolchuk, Yurii Ivanov (2021). Motivational Preconditions of Specialist Leadership Development in the Process of Training. Journal of Higher Education Theory and Practice. 2021. Vol. 21 (14). P. 183–190. DOI: https://doi.org/10.33423/jhetp.v21i14.4821.

5. Донець О. І., Шміголь Д. О. Патологічні зміни фізичного і психічного здоров'я військовослужбовців під впливом екстремальних умов // Молодий вчений. 2017. № 4. С. 232–236.

6. Леонтьев Д. А., Рассказова Е. И. Жизнестойкость как составляющая личностного потенциала. Личностный потенциал: структура и диагностика. М.: Смысл, 2011. 680 с.

7. Маслоу А. Новые рубежи человеческой природы / Пер. с англ. 2-е изд., испр. М.: Смысл: Альпина нон-фикшн, 2011. 425 с.

8. Building Psychological Resilience in Military Personnel: theory and practice / edited by Robert R. Sinclair and Thomas W. Britt. Washington, 2013.

9. Чорний В. С. Як повернути сержанту реальний авторитет // Філософська і соціологічна думка. 1993. № 9–10. С. 72–78.

10. Чорний В. С. Військова організація України: становлення та перспективи розвитку: монографія. Ніжин: ТОВ "Видавництво "Аспект-Поліграф", 2009. 368 с.

11. Шелухіна О. М. Психотренінгові технології розвитку психологічної стійкості працівників транспортної міліції // Науковий вісник Львівського державного університету внутрішніх справ. Серія психологічна. 2012. Вип. 2 (1). С. 338–346.

12. Combat and Operational Stress Control / Department of the NAVY. Washington, Headquarters United States Marine Corps, 2010. 221 p.

13. Promoting Psychological Resilience in the U.S. Military Published: [L. Meredith, C. Sherboume, and other.]. Santa Monica: RAND Corporation, 2011. 186 p.

14. Синишина В. М. Теоретико-методологічні проблеми формування психологічної стійкості фахівців рятувальних підрозділів МНС // Проблеми екстремальної та кризової психології. Ун-т цивільного захисту України. Вип. 10. Х.: НУЦЗУ. 2011. С. 164–171.

15. Bailey S. Canadian Forces Health Services Road To Mental Readiness Programme MCIF [military news publications] Surgeon General's Mental Health Strategy Canadian Forces Health Services Group, 2/2015. 65 p.

УДК: 621.396.49

Штонда Р. М. ORCID: 0000-0001-5986-0847 (ВІТІ ім. Героїв Крут)
Кузнецов В. М. ORCID: 0009-0009-6824-9308 (НУОУ)
Гоменюк В. М. ORCID: 0009-0007-2286-6832 (НУОУ)
Поліщук С. А. ORCID: 0009-0006-9110-7576 (НУОУ)
Підкова О. І. ORCID: 0009-0009-0387-7100 (НУОУ)

ОСОБЛИВОСТІ ВИКОРИСТАННЯ МАЛОГАБАРИТНИХ СТАНЦІЙ ТРОПОСФЕРНОГО ЗВ'ЯЗКУ В СУЧАСНИХ РЕАЛІЯХ

Властивості тропосферного зв'язку, які визначаються характером поширення радіохвиль, що в змозі надати прийнятні швидкості передачі, скритність та захищеність, незалежність функціонування лінії тропосферного зв'язку від характеру бойових дій, погоди, геомагнітної активності, високотних ядерних вибухів та мобільність, забезпечують йому належне місце серед інших родів зв'язку в системі електронних комунікацій.

Сучасні реалії показують, що використання високоточної зброї у поєднані із розвідувальними засобами, диверсійними групами, незаконними збройними формуваннями, радіоелектронною розвідкою, засобами радіоелектронної боротьби, сильно впливає на організацію та функціонування системи зв'язку. Дана тенденція із кожним роком тільки буде нарощуватися та удосконалюватися, що призведе до виникнення проблем із роботою систем зв'язку.

Останніми роками науковцями ведеться дискусія про роль та місце станцій тропосферного зв'язку в системі військового зв'язку. Ведення операцій (бойових дій) показало, що використання великогабаритних станцій тропосферного зв'язку призводить до моментального їх виявлення, а виявивши їх, противник вживає різноманітних заходів щодо їх знищення. Тому з'явилась актуальна задача щодо створення та впровадження малогабаритних станцій тропосферного зв'язку, які одночасно могли б поєднувати тропосферну та радіорелейну станцію зв'язку.

Проаналізувавши наукові видання за декілька останніх років, що стосуються тропосферного зв'язку, було з'ясовано, що переважно вони зорієнтовані на відображення принципів застосування та впровадження великогабаритних станцій тропосферного зв'язку вітчизняних виробників, а от за підходи до застосування малогабаритних станцій тропосферного зв'язку майже нічого не відображено.

Тому в статті авторами запропоновано підходи щодо застосування малогабаритних станцій тропосферного зв'язку та надані пропозиції щодо подальших напрямків наукової діяльності з розвитку тропосферного зв'язку.

Ключові слова: *малогабаритна станція тропосферного зв'язку, тропосферний зв'язок, радіорелейний зв'язок, супутниковий зв'язок, комбінована тропосферна-радіорелейна станція зв'язку, кібератака.*

R. Shtonda, V. Kuznetsov, V. Homeniuk, S. Polishchuky, O. Pidkova Features of the use of small-dimensional tropospheric communication stations in modern realities.

The properties of tropospheric communication, which are determined by the nature of the propagation of radio waves, which are able to provide acceptable transmission speeds, stealth and security, the independence of the functioning of the tropospheric communication line from the nature of hostilities, weather, geomagnetic activity, high-altitude nuclear explosions, and mobility provide it with its proper place among other types of communication in the electronic communications system.

Modern realities show that the use of high-precision weapons in combination with reconnaissance means, sabotage groups, illegal armed formations, radio-electronic intelligence, means of radio-electronic warfare, strongly affects the organization and functioning of the communication system. This trend will be only increasing and improving every year, which has lead to problems with the operation of communication systems.

In recent years, scientists have been debating the role and place of tropospheric communication stations in the military communication system. The conduct of operations (combat operations) has shown that the use of large-sized tropospheric communication stations leads to their immediate detection, and upon detecting them, the enemy takes various measures to destroy them. Therefore, there was an urgent task of creating and implementing small-sized tropospheric communication stations, which at the same time could combine a tropospheric and a radio relay communication station.

After analyzing the scientific publications for the last several years, related to tropospheric communication, it was found that they are mainly focused on reflecting the principles of application and implementation of large-sized tropospheric communication stations of domestic manufacturers, and on approaches to the use of small-sized tropospheric communication stations almost nothing is displayed.

Therefore, in the article, the authors proposed approaches to the use of small-sized tropospheric communication stations. And suggestions are provided regarding further directions of scientific activity in the development of tropospheric communication.

Keywords: *small tropospheric communication station, tropospheric communication, radio relay communication, satellite communication, combined tropospheric radio relay communication station, cyberattack.*

Постановка завдання в загальному вигляді. Протягом останніх років в науковому середовищі ведеться дискусія про роль та місце станцій тропосферного зв'язку в системі зв'язку. На сьогодні з'явилась актуальна задача створення та впровадження малогабаритних станцій тропосферного зв'язку (далі – МСТЗ), які одночасно могли б працювати в двох режимах: загоризонтного зв'язку та прямої видимості. Поєднання цих двох режимів в одному виробі дозволило б застосовувати станції тропосферного зв'язку під час ведення сучасних операцій (бойових дій) на полі бою з метою забезпечення надійного, стійкого, захищеного зв'язку між органами управління, зменшення ризиків щодо загибелі та травмування обслуговуючого персоналу та зниження можливості їх виявлення з метою ураження противником. Для досягнення даної мети буде необхідним впровадження в сучасну систему зв'язку МСТЗ.

Аналіз останніх публікацій. У роботі [1] проаналізовано недоліки існуючих вітчизняних мобільних засобів тропосферного зв'язку та сформульовано шляхи їхнього вдосконалення. Показано, що проблему розвитку військових систем цифрового тропосферного зв'язку необхідно вирішувати комплексно. Визначено напрямки вдосконалення мобільних засобів тропосферного зв'язку: створення станцій, що працюють за схемою «крапка – багато крапка»; розробка комбінованих та малогабаритних цифрових тропосферо-радіорелейних станцій.

У статті [2] запропоновано нові технічні рішення, ключові технології і концепція побудови конкурентоздатних малогабаритних станцій тропосферного зв'язку нового покоління з високою пропускною спроможністю і захищеним радіодоступом до каналів зв'язку. Показано, що на їхній основі в перспективі можна створити комбіновану станцію тропосферного і супутникового зв'язку.

У роботі [3] було досліджено стан, проблемні питання та напрямки подальшого розвитку вітчизняних тропосферних систем зв'язку. Автори розглядають технічні аспекти роботи тропосферних станцій у сучасних умовах та пропонують шляхи їхньої модернізації.

Отже, проведений аналіз основних публікацій показав, що на сьогодні є ряд статей та матеріалів досліджень стану тропосферного зв'язку в Збройних силах України, але не існує узагальнених робіт, які б всебічно розглядали підходи до застосування МСТЗ.

Метою статті є запропоновані підходи щодо застосування МСТЗ та надані пропозиції щодо подальших напрямків наукової діяльності з розвитку тропосферного зв'язку.

Виклад основного матеріалу. На сьогодні відомо про велику кількість кібератак на українські ресурси. 24 лютого 2022 року було запущено шкідливе програмне забезпечення AcidRain, яке видалило усі дані на модемах та маршрутизаторах Viasat, які на той час знаходились в роботі, через що всі термінали Viasat перестали забезпечувати супутниковий зв'язок. І саме таким методом були виведені з ладу тисячі терміналів.

Тому після порушення в роботі супутникового інтернет-сервісу Viasat велика частка передачі даних лягла на радіорелейні станції зв'язку [4]. Але на ряду із радіорелейними станціями зв'язку широко почали застосовуватися станції тропосферного зв'язку.

А отже одним із найбільш стійких та швидкісних способів передачі сигналу на сотні кілометрів, зокрема також у важкодоступні регіони, залишається тропосферний зв'язок.

Станції тропосферного зв'язку за своїм функціональним призначенням відносяться до каналоутворюючих станцій та призначені для будівництва (розгортання) ліній (осей, рокад, ліній прямого зв'язку між пунктами управління, ліній доступу (прив'язки)) та організації

каналів передачі інформації ними на стратегічному, оперативному та тактичному рівнях управління [5].

Станції тропосферного зв'язку розроблені десятки років тому, але після модернізації мають ряд переваг не тільки перед радіорелейними та супутниковими станціями зв'язку. Нині в Україні модернізовано ряд станцій тропосферного зв'язку, серед них Р-417 – до версії Р-417МУ та Р-423-1М – до версії Р-423-1МУ. Ці сучасні модернізовані станції відносяться до великогабаритних станцій тому, що обладнання розміщується в КУНГу, а КУНГ – транспортується транспортним засобом немалих габаритів та великою вантажопідйомністю, що не забезпечує скритість під час переміщень, розгортання та експлуатації станції тропосферного зв'язку [6].

Отже, необхідним постає питання в пошуку технічних рішень щодо зменшення великогабаритних станцій тропосферного зв'язку, а також уніфікації їхніх зовнішніх відмінних ознак, так як в умовах ведення операцій (бойових дій) будь-яка автомобільна техніка, що має нетипові ознаки, є об'єктом ураження. Тому для якісного виконання поставленого завдання щодо забезпечення надійного, стійкого, захищеного зв'язку, зменшення ризиків щодо загибелі та травмування обслуговуючого персоналу та зниження можливості їх виявлення з метою ураження противником, буде перехід від застарілих станцій тропосферного зв'язку на МСТЗ.

Для вирішення даного питання пропонується розглянути можливість застосування вітчизняних МСТЗ [7].

МСТЗ повинні бути створені по блочно-модульному принципу на базі єдиних уніфікованих конструкцій, розроблених із використанням сучасної мікроелектронної елементної бази та програмно-апаратних систем [8].

Основні складові конструктивні частини МСТЗ наведено на рисунку 1.

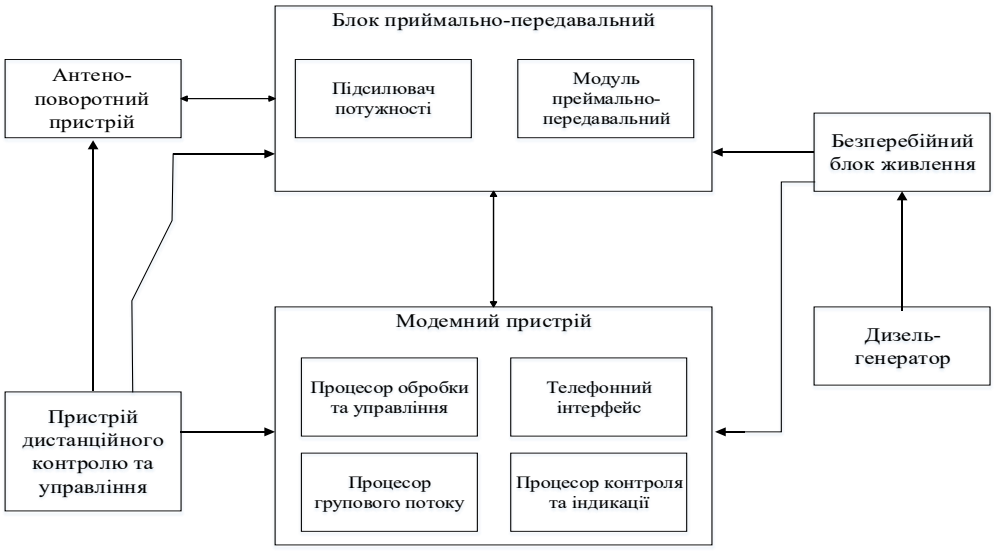

Рис. 1 Основні складові конструктивної частини МСТЗ

До складу антено-поворотного пристрою входять: тринога з можливістю встановлення обладнання вагою не менше 20 кілограм та механізмами закріплення на місцевості або на даху приміщень; антена радіусом не більше 1 метру; поворотний пристрій із забезпеченням повороту антени на 360 градусів.

До складу блоку приймально-передавального входять: підвищувальний конвертер частоти; підсилювач потужності з можливістю управління коефіцієнтом підсилення; дуплексні фільтри на передачу та прийом; малошумливий понижуючий конвертер частоти;

пристрій вбудованого автоматичного контролю виробу; елементи вторинного електроживлення вузлів виробу; перехід на антенний хвилевід круглого перерізу.

До складу модемного пристрою входять плати: блоку обробки та управління; процесора групового потоку і контролю та індикації; інтерфейсу телефонного; блоку вторинних джерел живлення; віддаленого підключення.

До складу пристрою дистанційного контролю та управління входить ноутбук з відповідними характеристиками та програмно-апаратним комплексом для налаштування МСТЗ; також повинна бути доступна функція віддаленого доступу керування та налаштування за допомогою смартфона/планшета.

Телекомунікаційний комплект ТК ТИП-3 у разі потреби ураховується можливість додавання ТК ТИП-4.

Засоби захисту інформації та кібербезпеки.

Джерело безперебійного живлення вихідною потужністю не менше 1500 Вт, діапазоном вхідної напруги живлення 160–295 В, вихідною номінальною напругою 230 В, не менше 12 годин неперервної роботи.

Дизель-генератор потужністю не менше 8 кВт.

Також до складу МСТЗ повинні входити кабелі живлення довжиною не менше 30 метрів, а також кабелі управління.

МСТЗ повинна мати наступні технічні характеристики: діапазон робочих частот від 4,4 ГГц до 5,0 ГГц; максимальна швидкість приймання/передачі цифрового інформаційного потоку до 8 Мбіт/с; інформаційний інтерфейс 10/100/1000 Base-T, наявні порти з можливістю інкапсуляції зовнішнього потоку конвертора E1 (G.703) в Ethernet; протокол та інтерфейс передачі даних IP (TCP/IP), Ethernet; вихідна потужність передавача на антенному фланці повинна бути приблизно 200 Вт; забезпечувати швидкість передачі даних до 100 Мбіт/с – при тропосферному зв’язку та до 200 Мбіт/с – при радіорелейному зв’язку; дальність тропосферної лінії зв’язку до 120 км; дальність радіорелейної лінії зв’язку до 40 км; час розгортання і входження в зв’язок повинен бути не більше 20 хв; можливість віддаленого управління повинно здійснюватися дистанційно на віддаленні не більше100 м.

Дане обладнання повинно бути виготовленим в захищеному виконанні за стандартом не нижче IP67. З урахуванням можливості живлення від декількох джерел. Одним із джерел живлення є стаціонарна (основна) мережа. У зв’язку з тим, що при живленні від стаціонарної мережі є можливість відбору значних величин потужності, а струмове навантаження зовнішніх силових кабелів і внутрішніх приводів обмежене, необхідно строго регламентувати споживану потужність, яка контролюється за показами споживаного струму. Так, номінальна величина споживаного струму для МСТЗ не повинна перевищувати величину 20–25 А. На нормальну роботу обладнання МСТЗ величина напруги живлення, яка повинна становити величину 220 В ± 10 % і постійно контролюватися.

За допомогою дизель-генератора (резервна мережа) МСТЗ може працювати у випадку відсутності стаціонарної мережі. У зв’язку з тим, що дизель-генератори розраховані на видачу обмежених величин потужності, живлення сторонніх споживачів заборонено.

У разі відсутності стаціонарної та резервної мережі обладнання МСТЗ може працювати від джерела безперебійного живлення. Безперервна робота повинна бути не менше 12 годин. При живленні від джерела безперебійного живлення категорично заборонено підключення сторонніх споживачі.

Обслуговуючий персонал/екіпаж, не більше ніж 3 чоловіка, повинен знати: свої ролі та за необхідністю замінити номер обслуги; досконало знати експлуатаційні можливості обладнання МСТЗ; уміти здійснювати розгортання обладнання МСТЗ у визначений термін; бути підготовленим та досконало знати принципи застосування МСТЗ; уміло проводити без порушень термінів технічне обслуговування МСТЗ.

Автомобільне шасі (пікап) формули 4×4 повинно забезпечувати надійну прохідність у різних кліматичних умовах на асфальтних та ґрунтових покриттях доріг, а також в важкодоступних складках місцевості. Залежно від умов проведення операцій (бойових дій) доцільно застосовувати броньоване автомобільне шасі з метою забезпечення збереження життя особового складу. Також для перевезення майна екіпажу необхідне доукомплектування броньованого автомобільного шасі одновісним чи двовісним напівпричепом з вантажопідйомністю не менше 3 тонн.

Для розрахунку зон доступу МСТЗ необхідно враховувати максимальне значення дальності, на яку буде здійснюватися передача сигналу за заданою швидкістю при необхідному значені якості передачі та заданою вірогідністю забезпечення зв'язку. Доступність каналу визначається за формулою (1) [9]:

$$P_c = P\left(P_{\text{прм}} \geq P_{\min}\right), \tag{1}$$

де $P_{\text{прм}}$ – потужність сигналу на вході прийомного пристрою;

$P_{\min}$ – реальна чутливість приймача;

$P_{\text{с}}$ – доступність каналу.

Розрахунок доступності каналу в зоні доступу повинен будуватися на розрахунку енергетичного потенціалу тропосферних ліній зв'язку.

Для розрахунку зон доступу на максимально допустимій відстані між МСТЗ у мережах необхідно враховувати:

потужності передавачів МСТЗ;

параметри антено-фідерного тракту прийому-передаючого обладнання (характеристики діаграм направленості антен, їхні діючі висоти, втрати в антено-фідерному тракті й ін.);

рівень зовнішніх та внутрішніх шумів на вході приймача та його чутливість;

електричні параметри обладнання, яке застосовується (робоча частота, тип модуляції, ширина полоси пропускання приймача й т. ін.).

Розглянуті параметри визначаються технічними умовами (технічними характеристиками) МСТЗ.

Максимальна зона доступу при високо піднятих антенах в умовах рівнинної місцевості визначається співвідношенням (2) [10]:

$$R_{\max} \leq 0{,}8\left[4{,}12\left(\sqrt{h_1} + 2\sqrt{h_0} + \sqrt{h_2}\right)\right], \tag{2}$$

де $R_{\max}$ – максимальна відстань до межі зони доступу;

h_1 – висота передавальної антени в метрах;

h_2 – висота прийомної антени в метрах;

h_0 – висота точки пересічення між напрямками випромінювання дотичних до поверхні землі антен.

Додаткові втрати вичислюються як (3) [10]:

$$W_{\text{дтр}} = W_{\text{ст}} + W_{\text{р}} + \Delta W_{\text{А}} + \Delta W_{\text{к}} + \Delta W_h + \Delta W_{hct} + \Delta W_{\text{з}}, \tag{3}$$

де $W_{\text{ст}}$ – стандартне ослаблення, яке залежить лише від відстані R і довжини хвилі λ;

$W_{\text{р}}$ – втрати, які обумовлені впливом нерівностей рельєфу місцевості і висот підйому антен;

$\Delta W_{\text{А}}$ – втрати підсилення антен;

$\Delta W_{\text{к}}$ – втрати, які обумовлені кліматичними умовами;

ΔW_{h} – втрати, які обумовлені впливом земної поверхні при невеликих величинах відношення h/λ;

$\Delta W_{\text{hст}}$ – втрати, які обумовлені відмінностями географічних висот;

$\Delta W_{\text{з}}$ – поправка, яка враховує швидкі та повільні завмирання.

Проведений розрахунок зон доступу МСТЗ, як зазначалось у виразах, дозволить обслуговуючому персоналу якісно будувати тропосферні лінії зв'язку.

Впровадження даних МСТЗ надасть можливість підвищити мобільність підрозділів зв'язку та якість виконання завдань.

Забезпечить:

стійкий та захищений зв'язок, який не залежить від погодних умов та фізичних перешкод, на відміну від супутникових станцій зв'язку;

високу завадозахищеність порівняно із супутниковими станціями зв'язку тих же діапазонів частот;

високу живучість порівняно з радіорелейними станціями зв'язку до дій наземних станцій перешкод та до станцій перешкод повітряного базування;

кращу протидію до направлених та загороджувальних перешкод;

можливість використання як тропосферної, так і радіорелейної станції зв'язку;

захищеність обслуговуючого персоналу/екіпажу.

Висновки. Отже, перспективність застосування МСТЗ, що відповідають тенденціям розвитку тропосферних і радіорелейних засобів зв'язку, є актуальним напрямком для розробки комбінованих цифрових комунікаційних систем. Вітчизняний науково-технічний та виробничий потенціал здатний вирішити питання імпортозаміщення в сфері військової техніки зв'язку і навіть в сфері тропосферного зв'язку.

Наступні напрямки науково-дослідних та дослідно-конструкторських робіт з розвитку МСТЗ слід направити на створення:

малогабаритних цифрових станцій тропосферного зв'язку;

комбінованих станцій тропосферного та радіорелейного зв'язку;

станцій тропосферного зв'язку, працюючих за схемою «крапка – багатокрапка».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Почерняєв В. М., Повхліб В. С. Стан і напрямки розвитку мобільних цифрових тропосферних систем зв'язку // Системи озброєння і військова техніка. ХНУПС ім. Івана Кожедуба. 2018. № 2 (54). С. 51–60.

2. Ільченко М. Є., Наритник Т. Н., Слюсар В. І. Напрямки створення тропосферних станцій нового покоління // Цифрові технології. К.: НТУУ КПІ. 2014. № 16. С. 8–18.

3. Масесов М. О., Субач І. Ю., Руденко Д. М., Станович О. В. Перспективи застосування цифрового діаграмоутворення у станціях тропосферного зв'язку спеціального призначення // Збірник наукових праць. Київ: ВІТІ ДУТ. 2014. № 1. С. 43–48.

4. Олексенко В. П., Штонда Р. М., Черниш Ю. О., Мальцева І. Р. Сучасні підходи до забезпечення кібербезпеки в радіорелейних лініях зв'язку // Кібербезпека: освіта, наука, техніка. Київ: КУ імені Бориса Грінченка. 2022. № 1 (17). С. 57–64.

5. Руденко В. І., Зінченко М. О., Бондаренко Л. О., Лазута Р. Р. Вибір і обґрунтування структури системи тропосферного зв'язку спеціального призначення з урахуванням застосування інноваційних технологій // Сучасні інформаційні технології у сфері безпеки та оборони. Київ: НУОУ. 2022. № 3 (45). С. 75–82.

6. Чайка Є. І., Штонда Р. М. Сучасні підходи до розвитку малогабаритних цифрових тропосферних станцій зв'язку // Перспективи розвитку та застосування сучасних систем і засобів зв'язку в інтересах управління військами: матер. наук.-практ. конф. Харків: НАНГУ, 2023. С. 10.

7. Кравчук С. О. Принципи створення портативних тропосферних радіорелейних станцій // Проблеми телекомунікацій: матер. Міжнар. наук.-техн. конф. Київ: НТУУ КПІ, 2015. С. 254–256.

8. Кравчук С. О. Портативна тропосферна радіорелейна станція зв'язку // Проблеми телекомунікацій: матер. Міжнар. наук.-техн. конф. Київ: НТУУ КПІ, 2016. URL: http://conferenc.its.kpi.ua/proc/article/view/70959 (дата звернення: 14.03.2023).

9. Руденок В. І., Бондаренко О. Є., Сергієнко А. В., Остапук О. І. Розрахунок зон доступу радіорелейними та тропосферними засобами зв'язку // Збірник наукових праць ВІТІ. 2018. № 3. С. 87–93.

10. Волков Е. А. Методика расчета радиорелейных и тропосферных линий связи / Е. А. Волков, В. П. Васильев, В. В. Куликов. Л.: ВАС, 1982.

АВТОРИ НОМЕРА

1. ***Атаманенко Микола Валерійович*** – молодший науковий співробітник науково-дослідної лабораторії Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

2. ***Білий Олександр Анатолійович*** – провідний науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

3. ***Бондаренко Олег Євгенійович*** – начальник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

4. ***Бригадир Сергій Петрович***– старший науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

5. ***Головко Олена Євгеніївна*** – науковий співробітник науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

6. ***Гоменюк Віктор Миколайович*** – слухач Національного університету оборони України, м. Київ, Україна.

7. ***Думітраш Вячеслав Олексійович*** – науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

8. ***Зінченко Михайло Олександрович*** – начальник науково-дослідного управління Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

9. ***Івченко Микола Миколайович*** – начальник проєктно-конструкторського відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

10. ***Карабань Олександр Валерійович*** – провідний науковий співробітник проєктно-конструкторського відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

11. ***Карпенко Андрій Олександрович*** – науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

12. ***Кокошинський Віталій Валєрійович*** – науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

13. ***Краснобокий Андрій Васильович*** – старший науковий співробітник науково-організаційного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

14. ***Кузнецов Віктор Миколайович*** – слухач Національного університету оборони України, м. Київ, Україна.

15. ***Куцаєв Володимир Вікторович*** – науковий співробітник науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

16. ***Лазута Роман Григорович*** – старший науковий співробітник науково-організаційного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

17. ***Лазута Роман Романович*** – начальник відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

18. ***Макарчук Василь Іванович*** – старший науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

19. ***Мусієнко Володимир Анатолійович*** – старший науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

20. ***Османов Руслан Нарімanович*** – начальник науково-дослідного відділу Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

21. ***Остапук Олександр Іванович*** – науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

22. ***Підкова Олександр Іванович*** – слухач Національного університету оборони України, м. Київ, Україна.

23. ***Плугова Ольга Богданівна*** – науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

24. ***Поліщук Сергій Анатолійович*** – слухач Національного університету оборони України, м. Київ, Україна.

25. ***Прохорський Сергій Ігорович*** – науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

26. ***Руденко Володимир Іванович*** – старший науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

27. ***Сергієнко Андрій Васильович*** – провідний науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

28. ***Сердюк Павло Євгенійович*** – науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

29. ***Тітаренко Андрій Володимирович*** – науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

30. ***Цимбал Ірина Володимирівна*** – науковий співробітник проєктно-конструкторського науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

31. ***Чорний Віталій Сергійович*** – професор кафедри Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

32. ***Штонда Роман Михайлович*** – начальник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

33. ***Шугалій Ольга Олександрівна*** – старший науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

34. ***Яковчук Олександр Вікторович*** – начальник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, м. Київ, Україна.

ПАМ'ЯТКА АВТОРУ

Наукові статті у фахових виданнях повинні мати такі необхідні елементи:

постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями;

аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спирається автор, виділення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття;

формулювання мети статті (постановка завдання);

виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів (моделей та результатів моделювання);

висновки з дослідження з визначенням наукової новизни;

перспективи подальших досліджень автора у даному напрямку.

Список використаних джерел повинен містити не менше 10–15 посилань бажано терміном видання не більше 10 років.

Рукопис подається у текстовому редакторі – **Microsoft Word 10 (не нижче).**

Формат аркуша – **А4 (210 мм × 297 мм).**

Розмір полів: зліва – **20 мм,** справа – **20 мм,** зверху – **20 мм,** знизу – **20 мм.**

Стиль – **normal** (звичайний), інтервал між рядками – **1,0,** абзацний відступ – **1 см.** Шрифт – **Times New Roman,** розмір шрифту – **12 пт,** із виключенням переносів.

Анотацію друкують курсивом, шрифт – **Times New Roman,** розмір шрифту – **10 пт.** Анотацію та ключові слова подають українською й англійською мовами. Обсяг кожної анотації з ключовими словами – **1800 знаків** із пробілами. Анотація повинна бути структурована так: вступ, проблематика, мета, матеріали й методи, результати, висновки. Іншими словами, анотація повинна відображати послідовну логіку опису результатів, описувати основну мету дослідження та підсумовувати найбільш значимі результати. Скорочення слів в анотації не застосовувати.

Після кожної анотації подають 5–7 ключових слів українською й англійською мовами відповідно. Список використаних джерел оформляється шрифтом 11 пт, згідно з ДСТУ 8302:2015 Інформація та документація. Бібліографічне посилання.

Не приймаються праці, у яких відсутній повний опис наукових результатів, що засвідчує їх, достовірність, або в яких повторюються результати, опубліковані раніше в інших наукових працях, що входять до списку основних (Постанова ВАК України від 10.02.99 № 1 – 02/3).

Статті, які містять загальновідому науково-технічну інформацію, плагіат, не розглядаються й не друкуються.

Рукопис статті потрібно подавати разом із зазначеними документами українською мовою: *акт експертизи*; *довідка про автора (авторів).*

Редакційна колегія залишає за собою право вносити в рукопис зміни редакційного характеру.

Телефон для довідок: 256-22-37, 256-22-73, внутрішній 442-37, 442-73.

Електронна адреса для надання статей: **naukaviti@gmail.com, naukaviti@viti.edu.ua.**

Етапи представлення статті для науковців інституту:

1. Стаття подається на розгляд головному редактору та після погодження – відповідальному редактору.

2. Після позитивного розгляду редколегією стаття подається коректору (кімната № 5 редакційно-видавничого відділу) для вичитки та корегування.

Виправлення електронного варіанта статті.

Друкування виправленого варіанта статті, отримання розпису коректора про виправлення помилок, що були виявлені, на останньому аркуші статті.

3. Виправлена стаття передається разом із супровідними документами відповідальному редактору для формування комп'ютерного макета збірника.