

ISSN 2524-0056 (Print)
ISSN 2519-481X (Online)

**ВІЙСЬКОВИЙ ІНСТИТУТ КИЇВСЬКОГО НАЦІОНАЛЬНОГО
УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА**

ЗБІРНИК НАУКОВИХ ПРАЦЬ

**ВІЙСЬКОВОГО ІНСТИТУТУ КИЇВСЬКОГО НАЦІОНАЛЬНОГО
УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА**

Виходить 4 рази на рік

№ 88

Згідно з наказом МОН №1188 від 24.09.2020, п. №156 Додатку 5 «Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка» включено до категорії «Б» за спеціальностями:

- F4 Системний аналіз та наука про дані (124);
- F6 Інформаційні системи і технології (126);
- K6 Забезпечення військ (сил) (254);
- K7 Озброєння та військова техніка (255).

**MILITARY INSTITUTE OF TARAS SHEVCHENKO NATIONAL
UNIVERSITY OF KYIV**

COLLECTION OF SCIENTIFIC WORKS

**OF THE MILITARY INSTITUTE OF TARAS SHEVCHENKO
NATIONAL UNIVERSITY OF KYIV**

It comes out 4 times a year

№ 88

According to the Order of the Ministry of Education and Science No. 1188 from 09/24/2020, item No. 156 of Appendix 5 «Collection of scientific works of the Military Institute of Taras Shevchenko National University of Kyiv» is included in category «B» by specialties:

F4 System analysis and date scsence (124);

F6 Information systems and technologies (126);

K6 Supply of troops (forces) (254);

K7 Armament and military equipment (255).

KYIV – 2025

УДК 621.43

ББК 32-26.8-68.49

Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, 2025. № 88. 154 с.

Голова редакційної колегії:

Лєнков С.В.

доктор технічних наук, професор, ВІКНУ;

Члени редакційної колегії:

Анісімов А.В.

доктор фізико-математичних наук, професор, член-кор. НАНУ, КНУ;

Барабаш О.В.

доктор технічних наук, професор, НТУУ КПІ;

Гунченко Ю.О.

доктор технічних наук, професор, ОНУ;

Жиров Г.Б.

кандидат технічних наук, старший науковий співробітник, КНУ;

Заславський В.А.

доктор технічних наук, професор, КНУ;

Карпінський М.П.

доктор технічних наук, професор, УНТ, Краків (Польща)

Лепіх Я.І.

доктор фізико-математичних наук, професор, ОНУ;

Петров О.С.

доктор технічних наук, професор, УНТ, Краків (Польща);

Погорілий С.Д.

доктор технічних наук, професор, КНУ;

Толок І.В.

кандидат педагогічних наук, доцент, НУЦЗУ;

Хайрова Н.Ф.

доктор технічних наук, професор, Університет Умеа (Швеція);

Хлапонін Ю.І.

доктор технічних наук, професор, КНУБА;

Шаронова Н.В.

доктор технічних наук, професор, НТУ ХП.

Редакційна колегія прагне до покращення змісту та якості оформлення видання і буде вдячна авторам та читачам за висловлювання зауважень і побажань.

Зареєстровано Міністерством юстиції України, свідоцтво про державну реєстрацію друкованого засобу масової інформації – серія КВ № 11541 – 413Р від 21.07.2006 р.

Відповідно до наказу МОН України від 24.09.2020 № 1188 «Збірник наукових праць ВІКНУ імені Тараса Шевченка» внесено до категорії «Б» (технічні науки).

Затверджено на засіданні Вченої ради ВІКНУ від 16.10.25 р., протокол № 3.

Відповідальна за макет:
Зарицька А.І.

Відповідальність за новизну і достовірність наведених результатів, тактико-технічних та економічних показників і коректність висловлювань несуть автори. Точка зору редколегії не завжди збігається з позицією авторів. Усі матеріали надруковані в авторській редакції.

Усі статті, що публікуються в збірнику, проходять обов'язкове рецензування, яке здійснюється за анонімною формою як для авторів, так і для рецензентів. Незважаючи на перевірку статей на антиплагіат, остаточну відповідальність за плагіат несуть автори.

Видання безкоштовне.

Примірники збірників знаходяться у: Національній бібліотеці України ім. В.І. Вернадського, науковій бібліотеці ім. М. Максимовича, бібліотеці Військового інституту та в наукових бібліотеках України згідно зі списком МОН. Електронна версія збірника розміщена на відповідних сайтах.

Видання індексується Google Scholar.

ОМ

Адреса редакції: 03189, м. Київ, вул. Ю. Здановської, 81, тел./факс +38 (044) 521 – 33 – 82

Наклад 50 прим. Ел. адреса редактора: lenkov_s@ukr.net

Офіційний сайт журналу: <http://miljournals.knu.ua>

Chairman of the editorial board:

Lienkov S.V. doctor of technical sciences, professor, VIKNU;

Members of the editorial board:

Anisimov A.V. doctor of physics and mathematics, professor, corresponding member of NASU, KNU;
Barabash O.V. doctor of technical sciences, professor, NTUU KPI;
Gunchenko Yu.O. doctor of technical sciences, professor, ONU;
Zhyrov G.B. candidate of technical sciences, senior researcher, KNU;
Zaslavsky V.A. doctor of technical sciences, professor, KNU;
Karpinski M.P. doctor of technical sciences, professor, UNT, Krakow (Poland)
Lepikh Ya.I. doctor of physics and mathematics, professor, ONU;
Petrov O.S. doctor of technical sciences, professor, UNT, Krakow (Poland);
Pogorilyy S.D. doctor of technical sciences, professor, KNU;
Tolok I.V. candidate of pedagogical sciences, docent, NUCP
Khairova N.F. doctor of technical sciences, professor, Umea University (Sweden);
Khlaponin Yu.I. doctor of technical sciences, professor, KNUBA;
Sharonova N.V. doctor of technical sciences, professor, NTU KhPI.

The editorial board strives to improve the content and quality of the publication and will be grateful to the authors and readers for their comments and wishes.

Registered by the Ministry of Justice of Ukraine, certificate of state registration of printed mass media – KV series No. 11541 – 413P from 07/21/2006.

In accordance with the Order of the Ministry of Education and Science of Ukraine from September 24, 2020 No. 1188, «Collection of Scientific Works of the Military Institute of Taras Shevchenko National University of Kyiv» is included in category «B» (technical sciences).

Approved at the meeting of the Scientific Council of VIKNU from 16.10.2025, prot. №3

Responsible for the layout:
Zaritsky A.

The authors are responsible for the novelty and reliability of the given results, tactical-technical and economic indicators and the correctness of statements. The point of view of the editorial board does not always coincide with the position of the authors. All the materials are printed in the author's edition.

All articles published in the collection undergo a mandatory review, which is carried out anonymously for both authors and reviewers. Despite checking the articles for anti-plagiarism, the final responsibility for plagiarism lies with the authors.

The publication is free.

Copies of the collections are in the National Library of Ukraine named after V.I. Vernadsky, in the scientific library named after M. Maksymovych, in the library of the Military Institute and in the scientific libraries of Ukraine according to the list of the Ministry of Education and Science. The electronic version of the collection is posted on the relevant websites.

The publication is indexed by Google Scholar.

Address of the editorial office: 03189, Kyiv, str. Y. Zdanovska, 81, phone/fax +38(044) 521 – 33 – 82 Edition of 50 copies. E-mail address of the editor: lenkov_s@ukr.net
Official website of the journal: <http://miljournals.knu.ua>

ЗМІСТ

ВІЙСЬКОВА ТЕХНІКА І ТЕХНОЛОГІЇ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

Зайцев І.П., Литвиненко Н.І., Єременок С.В., Сажко Ю.О. Тактичні особливості застосування короткоствольної стрілецької зброї в умовах обмеженого простору	7
Луцишин А.М., Лоза В.М., Василенко Є.Ю., Кондратюк В.В. Цифрові технології в формуванні методики оцінювання бойової ефективності використання короткоствольної стрілецької зброї	21
Кольцов Р.Ю., Левінськова Н.В., Кучер А.О. Розвиток артилерійської тактики у локальних та масштабних конфліктах	33
Попов С.А., Ленков С.В., Коновалюк М.Д. Методичні засади підготовки стрільби з використанням стрілецької зброї в урбанізованих середовищах	45

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Lienkov S.V., Haisha O.O., Lenkov Y.S., Haisha O.O. Application of Fuzzy Logic Methods to Develop a Quadcopter Landing Control System	59
Бобок І.І., Кобозєва А.А. Архітектура «нульової довіри» і перспективи її впровадження в державний сектор України	68
Бобровнікова К.Ю., Гурман І.В., Чорненький В.І., Муляр І.В. Метод та алгоритми виявлення кібератак у мережах інтернету речей на основі аналізу	82
Міночкін А.І., Кузавков В.В., Романенко М.М. Передавальна функція розімкненої системи автоматичного управління з гідроприводом	95
Хлапонін Ю.І., Кондакова А.М. Дослідження ефективності розроблених алгоритмів та моделей захисту в мережах інтернету речей	103

ЗАГАЛЬНІ ПИТАННЯ

Акімов О.О., Золотов А.В., Андрусяк М.В., Русецький Р.Ю. Аналіз досвіду формування військового законодавства щодо проходження військової служби у збройних силах Ізраїлю	114
Князєв С.М., Крилов С.А., Ємцов А.А. Дієва оцінка системи кадрового менеджменту Збройних Сил України	126
Маміч В.В., Максименко Ю.А., Дідик В.О., Буз А.В., Шерстюк А.Д. Аналіз перспективних методів аналітичної діяльності військових фахівців	137

Дані про авторів	142
Алфавітний покажчик	144
Редакційна політика та етичні норми	145
Якісні показники членів редакційної колегії.	147
Порядок подання і оформлення статей до «Збірника наукових праць Військового інституту Київського національного університету імені Тараса Шевченка»	148

CONTENTS

MILITARY EQUIPMENT AND TWO-DESTINATION TECHNOLOGIES

Zaitsev I.P., Lytvynenko N.I., Ieremenok S.V., Sazhko Y.O. Tactical features of using short-barreled firearms in confined spaces	7
Lutsyshyn A.M., Loza V.M., Vasylenko Y.Y., Kondratiuk V.V. Digital technologies in developing a methodology for assessing the combat effectiveness of short-barreled small	21
Koltsov R.U., Levinskova N.V., Kucher A.O. Development of artillery tactics in local and large-scale conflicts	33
Popov S. A., Lienkov S.V., Konovaliuk M.D. Methodological principles of shooter training and the use of small arms in urban environments	45

INFORMATION TECHNOLOGIES

Lienkov S.V., Haisha O.O., Lenkov Y.S., Haisha O.O. Application of Fuzzy Logic Methods to Develop a Quadcopter Landing Control System	59
Bobok I.I., Koboziyeva A.A. Zero trust architecture and prospects for its implementation in the government sector of Ukraine	68
Bobrovnikova K.Yu., Hurman I.V., Chornenkyi V.I., Muliar I.V. Research on the effectiveness of developed algorithms and protection models in internet of things networks	82
Minochkin A.I., Kuzavkov V.V., Romanenko M.M. Transfer function of an open-circuit automatic control system with hydraulic drive	95
Khlaponin Yu.I., Kondakova A.M. Research on the effectiveness of developed algorithms and protection models in internet of things networks	103

GENERAL QUESTIONS

Akimov O.O., Zolotov A.V., Andrusiak M.V., Rusetskyi R.U. Analysis of the experience of forming military legislation on military service in the Israel Defense Forces	114
Kniaziev S.M., Krylov S.A., Yemtsov A.A. Effective assessment of the personnel management system in the Armed Forces of Ukraine	126
Mamich V.V., Maksimenko Yu.A., Didyk V.O., Buz A.V., Sherstyuk A.D. Analysis of prospective methods of analytical activity of military specialists	137

Data on Authors	142
Alphabetical Index	144
Editorial policy and ethical standard	145
The order of submission and registration of articles to the "Collection of scientific works of the Military Institute of the Taras Shevchenko National University of Kyiv "	148

ВІЙСЬКОВА ТЕХНІКА І ТЕХНОЛОГІЇ ПОДВІЙНОГО ПРИЗНАЧЕННЯ

УДК: [355.48+623.44]:355.58

док. філос., доц. **Зайцев І.П.** (ВА м. Одеса)
к.т.н, с.н.с. **Литвиненко Н.І.** (ВІКНУ)
Єременок С.В. (ВА м. Одеса)
Сажко Ю.О. (ВА м. Одеса)

DOI: <http://doi.org/10.17721/2519-481X/2025/88-01>

ТАКТИЧНІ ОСОБЛИВОСТІ ЗАСТОСУВАННЯ КОРОТКОСТВОЛЬНОЇ СТРІЛЕЦЬКОЇ ЗБРОЇ В УМОВАХ ОБМЕЖЕНОГО ПРОСТОРУ

Стаття присвячена вивченню тактичних особливостей застосування короткоствольної стрілецької зброї в умовах обмеженого простору, зокрема в урбанізованому середовищі, де ключовими факторами є швидкість реагування, маневреність і координація дій. Дослідження аналізує специфіку ближнього бою, акцентуючи на необхідності адаптації стрілецької підготовки до умов тісних приміщень. Мета статті – обґрунтувати методичні засади ефективного використання короткоствольної стрілецької зброї в обмеженому просторі, сформулювати критерії оцінювання її бойової ефективності та запропонувати рекомендації для вдосконалення програм тактичної підготовки особового складу. Використано аналіз літературних джерел з тактики ближнього бою, технічних характеристик зброї та методик стрілецької підготовки, а також емпіричні дані, отримані шляхом моделювання бойових сценаріїв у тренувальних модулях типу «kill house». Дослідження включає тестування зброї на точність, швидкість реакції, ергономіку та безпечність у спеціально створених умовах, що імітують реальні бойові ситуації. Встановлено, що короткоствольна зброя, зокрема пістолети, забезпечує високу ефективність у ближньому бою завдяки компактності, швидкості приведення до бою та можливості стрільби в нестандартних положеннях, що є критично важливим у тісних приміщеннях. Запропоновано комплексну систему оцінювання, яка охоплює точність, швидкість, ергономіку, тактичну безпечність і психофізіологічну стійкість стрільця, що дозволяє об'єктивно визначити бойову спроможність. Наукова новизна полягає у формалізації тактичних алгоритмів для індивідуальних і групових дій, а також у розробці вправ, які враховують специфіку обмеженого простору, зокрема позиційну стрільбу та техніку входу в приміщення. Результати дослідження підкреслюють важливість інтеграції психофізіологічної підготовки та моделювання стресових умов для підвищення ефективності стрільців. Подальші дослідження можуть бути зосереджені на інтеграції технологій віртуальної та доповненої реальності для створення реалістичних тренажерних комплексів, що імітують бойові умови. Також перспективним є вивчення впливу новітніх прицільних систем і допоміжного обладнання на підвищення точності та швидкості стрільби в обмеженому просторі.

Ключові слова: короткоствольна зброя, ближній бій, обмежений простір, тактична підготовка, оцінювання ефективності, стрілецька підготовка.

Вступ та постановка проблеми. Специфіка ведення бойових дій, особливо в моделі урбанізованого простору, характеризуються високою щільністю забудови, численними внутрішніми приміщеннями, технічними зонами, вузькими проходами та іншими обмеженнями, які суттєво впливають на можливості застосування класичних видів зброї та маневру особового складу. В подібних обставинах короткоствольна стрілецька зброя набуває особливої тактичної ваги, оскільки забезпечує максимальну маневреність, оперативність реагування та зручність використання в обмеженому просторі. Її застосування є критично важливим під час зачистки приміщень, ведення ближнього бою в умовах обмеженої оглядовості та високої динаміки загроз. Водночас ефективність бойового використання короткоствольної зброї значною мірою залежить від відповідності її характеристик

конкретним умовам тактичного середовища, рівня підготовки стрільця, методів навчання та впровадження стандартизованих методик оцінювання. Наголос робиться на розробленні комплексного підходу до оцінювання її практичної придатності у ситуаціях, що моделюють реальні бойові сценарії, зокрема, у тісних приміщеннях, де обмежена можливість маневру та зростає ризик перехресного вогню. У цьому форматі дослідження проблематики тактичних аспектів застосування короткоствольної зброї в обмеженому просторі має як теоретичне, так і практичне значення для військової науки, підготовки особового складу та удосконалення сучасних програм бойової стрілецької підготовки.

Аналіз останніх наукових досліджень і публікацій. У працях ряду авторів [1-13] акцент зроблено на важливості технічних характеристик зброї: довжина ствола, ємність магазину, ергономіка – які безпосередньо впливають на її ефективність у ближньому бою. Проте часто автори дещо обмежуються описом загальних параметрів озброєння без глибокого аналізу специфіки його застосування в умовах обмеженої маневровості, що спостерігається в урбанізованому середовищі. Значну увагу в літературі приділено методикам підготовки до ближнього бою (CQB), які широко висвітлюються в роботах закордонних військових інструкторів і фахівців як то [4], [11], [14], однак їх підходи часто базуються на практичному досвіді без формалізації у вигляді системного оцінювання ефективності стрільця чи зброї. На цій основі ми констатуємо, що окреслена проблематика досі розглядається фрагментарно, а наявні напрацювання в галузі стрілецької підготовки потребують адаптації до сучасних бойових реалій.

Метою статті є: обґрунтування методичних засад ефективного бойового використання короткоствольної стрілецької зброї в обмеженому просторі з урахуванням специфіки ближнього бою.

Виклад основного матеріалу. У зв'язку з трансформацією характеру конфліктів, зростанням частки бойових зіткнень у містах, населених пунктах і закритих об'єктах критичної інфраструктури, зростає потреба у глибокому осмисленні та детальному аналізі особливостей застосування стрілецької зброї в умовах обмеженого простору. Некомфортне середовище має свої тактико-технічні характеристики, які істотно впливають на вибір типу зброї, тактику її використання, а також на підготовку особового складу. Передусім до обмеженого простору як тактичного середовища слід віднести такі типові елементи архітектурного середовища, як внутрішні приміщення будівель (житлових, адміністративних, промислових), вузькі коридори, сходові клітини, підвали, горища, технічні проходи, тунелі, шахти, а також транспортні засоби (залізничні вагони, автобуси, літаки, кораблі), де простір для дій стрільця суттєво обмежений фізичними перешкодами. В подібних умовах основною тактичною задачею є забезпечення швидкого і точного вогневого ураження цілі при мінімізації ризиків для самого стрільця, товаришів по групі та цивільного населення. Особливістю цього середовища є наявність великої кількості потенційних укриттів, тісного простору для маневру, обмеженого огляду та значної кількості «мертвих зон», що підвищує рівень тактичної складності кожної дії.

Короткоствольна зброя, зокрема пістолети, є оптимальним типом озброєння для виконання бойових завдань у таких умовах, оскільки поєднує в собі компактність, мобільність, швидкість приведення до бою та можливість ефективної стрільби з однієї руки. На відміну від довгоствольної зброї, яка потребує значного простору для маніпуляцій, короткоствольна дає можливість швидко реагувати на раптову загрозу навіть при суттєво обмеженій свободі рухів [3]. Крім того, при правильному використанні вона дає змогу зменшити ймовірність зачіпання стволом за перешкоди або випадкового контакту з іншим членом групи в процесі руху вузьким коридором чи зачистки приміщення (табл. 1).

Таблиця 1

**Оцінка впливу обмеженого простору на ефективність короткоствольної
стрілецької зброї Збройних Сил України [5]**

Тип зброї	Дистанція стрільби (м)	Точність в обмеженому просторі	Маневреність	Ефективність у ближньому бою
Пістолет (Форт-12)	10-25	Висока (компактний, зручний для прицілювання)	Відмінна (легкий, ергономічний)	Висока (надійний у ближньому бою)
Пістолет (Форт-17)	10-25	Висока (полімерна рама, точне прицілювання)	Відмінна (легший за Форт-12)	Висока (ефективний у тісних умовах)
Пістолет-кулемет (Форт-224)	20-50	Середня (розкид при швидкій стрільбі)	Хороша (компактний, але потребує вправності)	Висока (швидкострільність)
Укорочений автомат (АКС-74У)	50-100	Низька (складно прицілюватися в тісному просторі)	Середня (складаний приклад полегшує маневри)	Середня (громіздкість знижує ефективність)
Пістолет (ПМ, Макарова)	5-20	Висока (простота, надійність)	Відмінна (компактний, легкий)	Висока (ефективний у ближньому контакті)
Пістолет-кулемет (MP5)	25-50	Середня (зниження точності через габарити)	Хороша (зручний для швидких маневрів)	Висока (швидкий темп вогню)
Дробовик (Форт-500)	5-20	Низька (широкий розкид дробу)	Низька (габарити ускладнюють маневри)	Дуже висока (руйнівна сила на близькій відстані)

Проте обмежений простір суттєво ускладнює маневреність стрільця, знижуючи здатність до зміни позиції, ухилення, переміщення в обхід або відступ. Вузькі коридори не дозволяють виконувати флангові маневри, а наявність меблів, перегородок чи інших перешкод може призвести до блокування тіла або зброї. Окрім того, у випадку штурму приміщень або зачистки багатопверхових будівель, стрільцю часто доводиться вести вогонь під незвичними кутами, у нестійких положеннях (присід, лежачи, з коліна, стрільба через вікно, дверний проріз, отвір у стіні), що потребує не лише високої техніки володіння зброєю, а й попереднього тренування у подібних умовах. Огляд, як критичний фактор успішного вогневого контакту, в умовах обмеженого простору зазнає серйозних обмежень. У закритому середовищі поле зору стрільця різко звужується, особливо під час руху сходами або у вузьких проходах, де стіни, кути й арки блокують прямий візуальний контакт із ціллю. Ці фактори ускладнюють своєчасне виявлення супротивника, особливо якщо той перебуває у засідці, використовує елементи маскування або зливається з інтер'єром. Більше того, навіть короткочасна втрата орієнтації у просторі через дим, погане освітлення, шум або стресовий фактор, може призвести до фатального зволікання у прийнятті рішень.

Одним з найсерйозніших тактичних викликів є обмежене поле зору, що у поєднанні з високою динамікою цілі, тобто швидкою зміною її позиції, несподіваним з'явленням з-за перешкод чи із суміжного приміщення і вимагає від стрільця виняткової готовності до миттєвої реакції. Ближній контакт із противником передбачає стрільбу з мінімальних дистанцій (менше ніж 5 метрів), де рішення приймаються упродовж часток секунди. Саме тому тренування в умовах, що моделюють обмежений простір, має включати не лише вправи зі стрільби, а й розвиток просторово-часової орієнтації, інстинктивної стрільби, координації рухів і здатності діяти у стані підвищеного психофізіологічного навантаження. Ще одним обмеженням є нездатність стрільця використовувати повноцінну захисну позицію саме потім, у більшості випадків, він змушений стріляти стоячи або у напівзігнутому положенні, не маючи змоги ефективно укритися, що підвищує ризик поранення або загибелі. Саме з цієї причини короткоствольна зброя має бути не лише зручною і легкою, а й забезпечувати надійність у будь-яких умовах, зокрема при стрільбі в тісному контакті, через тканину, на близькій відстані до супротивника. Окремого розгляду потребують небезпеки, які виникають під час використання короткоствольної зброї в груповій тактиці. У тісному приміщенні легко створити ситуацію «перехресного вогню», коли стрільці несвідомо опиняються в лінії прицілу один одного. Координація, злагодженість дій, чітке дотримання секторальної відповідальності

кожного члена групи є критичними для уникнення «дружнього вогню». Тактична комунікація (словесна та жестова), попереднє відпрацювання сценаріїв та повторення процедур входу в приміщення, і усе це повинно бути інтегрованим елементом програми підготовки.

У практиці сучасної військової справи, де ключовими критеріями успішного виконання завдань все частіше виступають швидкість реагування, точність першого пострілу та ефективність ураження супротивника в умовах обмеженого простору, короткоствольна стрілецька зброя (у першу чергу – пістолети та револьвери) посідає вагомe місце в арсеналі засобів ближнього бою. Її застосування, хоча традиційно асоціюється з правоохоронною діяльністю та озброєнням особового складу допоміжних підрозділів, дедалі частіше включається до тактичних моделей сучасних збройних сил, зокрема під час проведення спеціальних операцій у населених пунктах, зачисток приміщень, конвоювання, охорони важливих об'єктів, патрулювання або дій у тилу противника. Головними характеристиками короткоствольної зброї, які визначають її переваги у ближньому бою, є компактність, ергономічність, швидкість приведення до бойового стану, а також зручність носіння в умовах прихованого або обмеженого доступу до повнорозмірного озброєння. Ефект компактності стає формою переваги стрільця та зберігати мобільність навіть у тісних приміщеннях, коридорах, транспортних засобах або під час руху серед щільної забудови, де застосування довгоствольної зброї ускладнене фізичними перешкодами, тісністю чи небезпекою зачепити стволом навколишні об'єкти. Здатність пістолета швидко діставатися, миттєво реагувати на загрозу шляхом пострілу однією рукою з будь-якої позиції є критичним фактором, особливо коли час реакції обмежується частками секунди, а від правильного першого руху залежить життя стрільця [8].

Короткоствольна зброя, зазвичай, характеризується простотою у використанні: механізми пістолетів та револьверів інтуїтивно зрозумілі, а сам процес заряджання, розряджання, зміни магазину або виконання пострілу можна виконувати в умовах недостатньої видимості або навіть під стресовим тиском. Значна частина сучасних пістолетів обладнана механізмами попереджувального натиску спуску, що підвищує безпечність у поводженні, а також можливістю встановлення лазерного прицілу чи тактичного ліхтаря, що полегшує виявлення та ідентифікацію цілі у темних або задимлених приміщеннях.

Порівнюючи короткоствольну і довгоствольну стрілецьку зброю в умовах тісного середовища, доцільно підкреслити принципову відмінність у маневреності, ергономіці й швидкості приведення до бою. Довгоствольна зброя, зокрема автомат чи карабін, незважаючи на вищу точність на середніх і дальніх дистанціях, значно поступається за зручністю у ситуаціях, коли стрілець змушений діяти у вузькому коридорі, обмеженому проході чи приміщенні з великою кількістю перешкод. Спроба використання довгоствольної зброї у таких умовах часто призводить до уповільнення часу реагування, підвищення ймовірності зачеплення стволом за навколишні об'єкти або неконтрольованого розвороту, що в бойовій ситуації може призвести до фатальних наслідків.

На противагу цьому, короткоствольна зброя забезпечує стрільцю необхідний рівень свободи дій у нестандартних положеннях тіла – наприклад, у положенні сидючи, напівлежачи, з-за дверного отвору чи вікна, або під час стрільби однією рукою при другій, зайнятій утриманням щита чи пораненого товариша. У багатьох випадках саме такий тип зброї стає основним засобом ураження супротивника в перші секунди контакту на ближній дистанції (1–5 метрів), що вимагає від неї максимальної надійності та здатності працювати у складних умовах – при пилу, вологості, обмеженому огляді, слабкому освітленні чи навіть при частковому блокуванні механізмів. Особливе значення у виборі короткоствольної зброї має вибір калібру, типу боєприпасів і конструктивних особливостей зброї. Найбільш поширеним калібром у військових та правоохоронних структурах залишається 9×19 мм Parabellum (Luger), який забезпечує оптимальне співвідношення між пробивною здатністю, віддачею та об'ємом магазину. Цей калібр є достатньо потужним для враження цілі на короткій дистанції, при цьому не створює надмірної віддачі, що може ускладнити повторну прицільну стрільбу, особливо при веденні вогню швидкими чергами [9].

У деяких випадках, зокрема під час виконання спеціальних завдань (контрдиверсійні операції, дії в густонаселених районах або при загрозі третім особам), можуть застосовуватись боєприпаси зі зменшеною пробивною здатністю, які мінімізують ризик рикошету чи наскрізного ураження сторонніх осіб. Наприклад, розширювальні кулі типу hollow point можуть використовуватись для зниження летальності за межами визначеної цілі. Проте важливо зауважити, що використання таких боєприпасів вимагає узгодження з міжнародними гуманітарними нормами та мандатом операції. Револьвери, хоч і втрачають популярність у військовому середовищі через меншу кількість набоїв у барабані та більший час на перезаряджання, залишаються актуальними в умовах, де ключовим є безвідмовність і простота механізму. Їх конструкція дозволяє вести вогонь у найекстремальніших умовах, коли пістолет із магазином може дати осічку або застрягнути через забруднення. Саме ц цих причин, револьвери досі використовуються в арсеналах окремих спецслужб як резервна зброя, особливо у ситуаціях, де життя стрільця залежить від одного точного пострілу. Що стосується конструктивних характеристик, до важливих параметрів відносяться довжина ствола (оптимально 90–120 мм), маса (не більше 1 кг без набоїв), форма руків'я (анатомічна, з антиковзким покриттям), наявність направляючої типу «Picatinny» для кріплення допоміжних засобів (ліхтар, лазерний цільовказівник), а також можливість швидкої розрядки і заміни магазину. Сучасні моделі типу Glock 17, SIG Sauer P226, CZ P-10 або Beretta APX широко використовуються у провідних арміях світу саме завдяки їхній відповідності цим вимогам. Необхідно також враховувати тактичний контекст, у якому застосовується короткоствольна зброя. У більшості випадків вона виконує роль резервного засобу вогневого ураження, який використовується після розрядження основної зброї або у випадку її втрати/несправності. Водночас для деяких категорій особового складу (пілоти, екіпажі бронетехніки, оператори радіоелектронної боротьби, розвідники) пістолет є основною зброєю, що зумовлює підвищені вимоги до його універсальності, надійності, легкості та інтуїтивної зручності у використанні [13].

У військовій справі, особливо в контексті сучасних бойових дій, що відзначаються стрімким зростанням інтенсивності ближнього вогневого контакту в урбанізованому середовищі, методика оцінювання ефективності застосування короткоствольної стрілецької зброї набуває ключового значення. Це зумовлено як необхідністю забезпечення високого рівня готовності особового складу до ведення бою в умовах тісного простору, так і потребою у стандартизованому, надійному й об'єктивному підході до перевірки спроможностей стрільця в критичних тактичних сценаріях. З огляду на це, системне опрацювання науково обґрунтованих критеріїв, методик та моделей випробування короткоствольної зброї є актуальним завданням не лише для інструкторсько-командного складу, а й для розробників озброєння, які орієнтуються на потреби сучасного бою ближнього контакту.

У першу чергу, ефективність застосування короткоствольної зброї має оцінюватися з урахуванням чотирьох базових критеріїв, які прямо впливають на бойову результативність стрільця: точність стрільби, швидкість ураження цілі, ергономічність та керованість зброї, а також безпечність її використання для самого стрільця і його тактичної групи. Кожен із цих критеріїв є багатовимірним і залежить як від технічних характеристик конкретного зразка зброї, так і від рівня підготовки користувача, фізіологічних і психологічних особливостей середовища, у якому ведеться стрільба [13].

Точність стрільби, як основоположний тактико-технічний параметр, в умовах обмеженого простору набуває особливого значення, оскільки стрільба часто ведеться в безпосередній близькості до цілі, з обмеженим часом на прицілювання і, нерідко, в нестандартних положеннях тіла. За такого порядку розвитку подій, доцільно забезпечити не лише точність першого пострілу, але й збереження допустимого рівня розсіювання куль при веденні швидкісної стрільби. Випробування мають включати вправи, що імітують реальні сценарії – стрільба з укриття, через дверний проріз, під кутом, або при раптовій появі цілі в полі зору. Контрольні показники можуть оцінюватися як за допомогою класичних мішеней (типу «силует»), так і із використанням інтерактивних систем з фіксацією траєкторій влучань.

Швидкість ураження цілі є другим важливим критерієм, що має бути вимірюваний у безпосередньому зв'язку з точністю. У ситуації ближнього бою, коли від моменту виявлення загрози до пострілу проходять секунди або навіть частки секунди, затримка зі сторони стрільця може стати фатальною. Оцінювання цього параметра доцільно здійснювати із застосуванням таймерів реакції, систем візуального та звукового запуску цілі, а також автоматизованих полігонів, де з моменту появи цілі до першого пострілу фіксується час з точністю до мілісекунд. У реальних умовах тактичного навчання такі вправи дозволяють виявити слабкі місця у техніці поводження зі зброєю, неправильні навички витягування чи приведення пістолета до бою, що критично важливо для покращення бойової готовності [12].

Керованість зброї та зручність у використанні, або так звана ергономіка, включає в себе здатність стрільця на інтуїтивному рівні утримувати контроль над зброєю під час стресу, стрільби у русі або в нестандартному положенні тіла. Для короткоствольної зброї цей аспект є вкрай важливим, оскільки саме зручність руків'я, вага зброї, баланс ствола, форма спускового гачка й легкість перезаряджання визначають, наскільки ефективно вона може бути застосована в реальних умовах. Методика оцінювання повинна включати як опитування суб'єктивних відчуттів стрільців, так і об'єктивні показники – точність під час повторного пострілу, швидкість перезарядки, кількість осічок або заїдань. Особливо важливим є тестування зброї у стресових умовах (імітація диму, шуму, зниження освітленості), які наближують ситуацію до реального бою.

Виділяємо критерій безпечності, який охоплює не лише механічну надійність зброї, а й тактичну безпечність її застосування в умовах обмеженого простору, зокрема – у складі групи. Під час дій в тісному середовищі, особливо в приміщеннях, легко порушити лінію секторів вогню, допустити перехресне наведення або спровокувати неконтрольований рикошет. Тому методика має враховувати наявність технічних рішень, що підвищують безпечність (наявність запобіжників, форм-фактор, що мінімізує можливість випадкового спрацювання), а також рівень вишколу стрільця у дотриманні правил безпечного поводження зі зброєю в колективному середовищі.

Для забезпечення об'єктивного тестування у реалістичних умовах, випробування короткоствольної зброї повинні проводитися у форматі сценаріїв, що моделюють дії у Close Quarters Battle (CQB) – ближньому бою у приміщеннях. Ці сценарії мають охоплювати наступні типові ситуації: штурм кімнати, зачистка коридору, стрільба з-за укриття, дії при виявленні супротивника у мертвій зоні, евакуація пораненого під вогнем, стрільба з різних рівнів (стоячи, з коліна, лежачи), використання другої руки, стрільба в умовах затемнення або під впливом шумових подразників. Всі випробування повинні проходити у спеціально облаштованих приміщеннях і так званих «kill house» або «штурмових модулях», які відтворюють архітектурну структуру житлових або промислових будівель [2].

У межах кожного сценарію фіксуються не лише кінцеві результати (кількість влучань, час виконання, кількість тактичних помилок), але й процесуальні показники – техніка входу в приміщення, координація з групою, контроль сектора обстрілу, точність першого пострілу, поведінка при осічці або зміні магазину. Бажано також фіксувати відеозапис дій стрільця з декількох ракурсів для подальшого розбору тактичних рішень. Для стандартизації підготовки та оцінювання ефективності застосування короткоствольної зброї, доцільно запроваджувати комплекс вправ і тестів, що можуть бути використані як під час базової підготовки, так і в процесі періодичного контролю навичок. Серед них [1, 8]:

– «Double Tap» – швидка стрільба двома пострілами по одній мішені, фіксація часу і розсіювання;

– «Mozambique Drill» – два постріли в корпус, один – у голову, на точність і швидкість;

– «Failure Drill» – вправа на зміну магазину після часткової осічки;

– «Room Entry Drill» – вхід у приміщення, виявлення і ураження кількох цілей;

– «Low-Light Reaction» – стрільба при слабкому освітленні з ліхтарем або нічним прицілом;

– «Injured Hand Drill» – стрільба з однієї руки, з імітацією поранення;

- «Shooting from Cover» – стрільба з-за укриття, зміна позицій;
- «Hostage Scenario» – стрільба по мішені з умовною «заручницею», оцінка точності.

Кожна вправа – це чіткі параметри виконання: допустимий час, допустимий відсоток влучань, технічні вимоги до безпеки, допустиму кількість тактичних помилок. Крім того, доцільно використовувати багаторівневу систему оцінювання – від базового (для новачків) до професійного (для спецпризначенців), що дозволяє диференціювати програму підготовки відповідно до категорії стрільців (табл. 2).

Таблиця 2

Оцінка ефективності короткоствольної зброї в умовах ближнього бою

Критерій	Опис	Методи оцінки	Ключові показники	Рекомендовані сценарії
Прицільна точність	Забезпечення влучності першого та наступних пострілів у обмеженому просторі	Стрілецькі вправи на мішенях типу «силует», інтерактивні системи фіксації траєкторій	Відсоток влучань, розсіювання куль (мм), стабільність при швидкісній стрільбі	Стрільба з укриття, через дверний проріз під кутом
Швидкість реакції	Час від виявлення цілі до першого пострілу в умовах стресу	Використання таймерів реакції, автоматизовані полігони з фіксацією часу до мілісекунд	Час до першого пострілу (мс), час виконання вправи	«Double Tap», «Mozambique Drill», «Room Entry Drill»
Ергономіка та контроль	Зручність утримання, баланс, легкість перезарядки та управління зброєю	Суб'єктивні опитування, тести на швидкість перезарядки, оцінка осічок	Час перезарядки (с), кількість осічок, точність повторного пострілу	«Failure Drill», «Injure Hand Drill», «Shooting from Cover»
Тактична безпечність	Надійність зброї та безпечність її використання в групі	Тести на запобіжники, аналіз рикошетів, оцінка дотримання секторів вогню	Кількість тактичних помилок, випадкові спрацювання	«Hostage Scenario», «Room Entry Drill», д. в групі
Адаптивність до умов	Ефективність стрільби в стресових умовах (шум, затемнення, рух)	Стрільба в «kill house» при низькому освітленні з шумовими подразниками	Точність у затемненні, координація в русі, час виконання	«Low-Light Reaction», «Shooting from Cover», евакуація пораненого
Тактична координація	Взаємодія стрільця з групою в умовах ближнього бою	Відеозапис сценаріїв CQB, аналіз техніки входу та контролю секторів	Кількість помилок координації, ефективність входу в приміщення	«Room Entry Drill», зачистка коридору, групові дії
Психофізіологічна стійкість	Здатність стрільця зберігати контроль під впливом стресу	Тести в умовах імітації бою (дим, шум, обмежений час), аналіз поведінки	Час реакції під стресом, точність у нестандартних умовах	«Low-Light Reaction», «Hostage Scenario», стрільба в русі

Отже, методика оцінювання повинна бути не просто набором критеріїв чи тестів, а цілісною системою, що охоплює теоретичні, практичні та психофізіологічні аспекти підготовки. Вона має включати оцінку точності та швидкості стрільби, рівня керованості зброї, безпечності дій в тісному тактичному середовищі, а також відповідати реальним сценаріям, що відображають характер сучасного бою. Ці засади об'єктивно виявляють видимі прогалини у підготовці, коригувати тактичні рішення, адаптувати вибір зброї та вдосконалювати програми навчання відповідно до оперативної обстановки та функціонального призначення підрозділів [12].

Традиційні моделі бойового зіткнення, побудовані на принципах відкритого бою, мають обмежене значення у контексті ближнього контакту в приміщеннях, де вирішальне значення набувають швидкість реагування, мінімізація профілю стрільця, здатність працювати у замкненому об'ємі та, найголовніше, синхронізація дій у межах штурмової або патрульної групи. Тому формування системного підходу до тактики застосування короткоствольної зброї в обмеженому просторі є одним із ключових завдань сучасної військової методики та практики бойової підготовки. Однією з базових категорій, яка охоплює сукупність тактичних

дій в умовах замкнутого простору, є позиційна стрільба, що передбачає виконання вогневого ураження цілі з фіксованого або частково мобільного положення, найчастіше – із використанням елементів навколишнього середовища як укриття. У ситуації, коли боєзйткнення відбувається у коридорі, кімнаті, технічному приміщенні або вузькому переході, стрілець повинен зайняти таку позицію, яка, з одного боку, забезпечує йому мінімальну вразливість для вогню супротивника, а з іншого – дозволяє контролювати простір у напрямку руху або передбачуваної загрози. Практика підтверджує, що найбільш ефективною є стрільба з-за кута із частковим висуненням зброї або руки (без повного відкриття тулуба), що дозволяє максимально використовувати переваги рельєфу або інтер'єру. Увагу слід тоді приділяти мінімізації експозиції: витягування лише пістолета, контроль нахилу голови, використання дзеркала або пристроїв віддаленого візуального огляду. У деяких ситуаціях позиційна стрільба супроводжується переміщенням між кількома точками вогневого контролю в межах приміщення або обмеженої зони, що дозволяє запобігти фіксації стрільця ворогом та ускладнює його прицілювання. Зміна позицій потребує динамічної координації з іншими членами групи та обов'язкового прикриття, адже в момент переміщення стрілець є найбільш вразливим [10].

Не менш важливою складовою тактики є робота в парі або в складі штурмової групи, що вимагає бездоганної координації дій, дотримання секторів стрільби, уникнення тактичних конфліктів у межах простору (зокрема, перехресного вогню), а також ефективної внутрішньої комунікації. Найбільш ефективною є модель, за якої кожен боєць має чітко закріплений сектор відповідальності, який покриває визначену зону (наприклад, правий кут приміщення, дверний проріз, сходовий проліт тощо). Застосування чітких команд, як голосових, так і візуальних сигналів (жестів), дозволяє у напруженій ситуації, яка супроводжується шумом, димом або обмеженою видимістю, підтримувати бойову цілісність групи. Уникнення перехресного вогню – критично важливий фактор: стрілець повинен не лише точно знати свій сектор, але й контролювати положення товаришів по команді, аби у процесі зачистки або реакції на загрозу уникнути випадкового влучання. Маємо підкреслити і необхідність проведення тренування спільного руху групи: проходження вузьких коридорів, синхронний вхід у приміщення, прикриття флангів, контроль тилу.

Наступним аспектом є техніка входу в приміщення, яка передбачає реалізацію швидких, скоординованих дій штурмової групи або окремого стрільця задля нейтралізації супротивника, що може перебувати у різних секторах огляду. Існують різні моделі входу – «criss-cross» (перехресний вхід), «button hook» (вхід з огином кута), «direct to point» (прямий вихід на ціль) тощо – кожна з яких має свою доцільність залежно від конфігурації приміщення, кількості доступних входів та характеру ймовірної загрози. Тактичний алгоритм включає кидок погляду на зону перед входом, різкий прорив у кімнату з негайним покриттям секторів, ідентифікацію цілей і в разі необхідності – вогневе ураження. У цьому контексті особливої ваги набуває так званий «кутовий вогонь» (corner shooting), коли стрілець виконує постріли з часткового укриття, не виходячи у повний контакт із потенційною ціллю. Такий вогонь потребує спеціальної підготовки, розвитку моторики стрільби однією рукою, а також контролю за лінією пострілу, оскільки зміщення осі вогню при «переломі» кута може спричинити рикошети або ураження товариша по групі [4].

Стрільба однією рукою є надзвичайно актуальним тактичним елементом у ситуаціях, коли друга рука використовується для відкриття дверей, утримання щита, пораненого або ліхтаря. При цьому від стрільця вимагається не лише впевнене володіння зброєю, але й здатність зберігати точність при зміненому балансі тіла, особливо якщо стрільба ведеться у русі або в момент переходу через перешкоди. Необхідним елементом є і включення у програму бойової підготовки спеціалізованих вправ на інстинктивну стрільбу, без попереднього прицілювання, із залученням лише «м'язової пам'яті» і реакції на світлові чи звукові стимули.

Визначальний контекст у методиці ведення бою в обмеженому просторі матиме стрільба в нестандартних положеннях, які виникають унаслідок специфіки архітектури приміщення,

тактичної ситуації або раптового падіння, поранення, втрати рівноваги. Стрільба з присідання, з коліна, з положення лежачи, напівлежачи, зі спини – усі ці варіанти повинні відпрацьовуватись під час навчань, оскільки саме вони є типовими при бою в тісному середовищі, де вертикальна позиція часто є недосяжною або смертельно небезпечною. Найскладнішою технікою вважається стрільба зі спини, коли стрілець змушений виконати прицілювання у перевернутому положенні, утримуючи зброю з обмеженою свободою руху. Такий тип стрільби вимагає вже високого рівня координації, розвиненої моторики й стійкої психофізіологічної підготовки (табл. 3).

Таблиця 3

Тактичні аспекти ведення бою в обмеженому просторі

Техніка дій	Головні навички	Ситуація застосування	Засадничі переваги	Можливі обмеження
Позиційна стрільба	Контроль укриття, мінімалізація профілю, точність з часткового висунення	Коридори, кути приміщень, вузькі проходи	Зниження вразливості, контроль простору	Обмежена мобільність, потреба в координації
Робота в штурмовій групі	Координація, розподіл секторів, невербальна комунікація	Зачистка приміщень, штурмові операції	Висока ефективність групи, прикриття	Ризик перехресного вогню, складність синхронізації
Техніка входу в приміщення	Швидкий прорив, покриття секторів, ідентифікація цілей	Вхід у кімнату, штурм укріпленої точки	Швидка нейтралізація загроз	Висока вразливість при вході, потреба в тренуванні
Стрільба однією рукою	М'язова пам'ять, баланс тіла, інстинктивна стрільба	Відкриття дверей, утримання ліхтаря, рух через перешкоди	Гнучкість дій, універсальність	Знижена точність, потреба в практиці
Стрільба в нестандартних положеннях	Координація, моторика, психофізична стійкість	Бій у тісному просторі, падіння, поранення	Адаптація до складних умов	Висока складність виконання, ризик втрат контролю
Пошук цілі в напівтемряві	Стрільба з тактичним ліхтарем, робота зі сліпими зонами	Нічні операції, задимлення, обмежена видимість	Ефективність у складних умовах	Ризик самодемаскації, потреба в спеціальному обладнанні

Крім зазначеного, у контексті бойових дій у приміщеннях доцільним є застосування техніки «пошуку цілі» у напівтемряві або при частковому затемненні, що моделює умови реального бойового контакту вночі, при пошкодженні освітлення або при використанні димових засобів. При цьому короткоствольна зброя, оснащена тактичним ліхтарем або лазерним вказівником, має перевагу в точності наведення, але вимагає навичок стрільби при миттєвому переключенні з джерела світла на ціль. Тактична школа повинна включати вправи з імітацією «сліпих зон», коли стрілець змушений діяти в умовах неповного огляду та обмеженого часу на ідентифікацію загрози [2].

Парадигма ведення бойових дій усе більшою мірою орієнтується на урбанізоване середовище, де характер зіткнень, маневру та вогневого контакту набуває надзвичайної щільності, швидкоплинності та залежності від здатності особового складу діяти ефективно в обмеженому просторі. За такого варіанту короткоствольна стрілецька зброя стає основним інструментом ураження противника на ближніх дистанціях, а ефективність її використання значною мірою залежить не стільки від технічних характеристик самої зброї, скільки від системної підготовки стрільця до дій у складному просторово-тактичному середовищі. Саме тому організація навчального процесу, що відображає реалії дій у приміщеннях, коридорах, на сходових клітинах та у транспортних засобах, є критично важливою для формування стійких, автоматизованих навичок, необхідних у бою на коротких дистанціях [7].

Насамперед, одним із ключових елементів бойової підготовки є створення або залучення спеціалізованої тренувальної інфраструктури, яка дозволяє максимально наблизити умови навчання до реального середовища бою в тісному просторі. Йдеться про використання макетів приміщень, які можуть мати як стаціонарний, так і мобільний характер, а також модульних полігонів типу «kill house», що дозволяють конструювати змінні конфігурації кімнат, проходів і перешкод відповідно до конкретного навчального сценарію. Всі типи об'єктів мають бути обладнані дверними отворами, вікнами, перегородками, сходовими прольотами, що створює

можливість моделювати реалістичні ситуації: штурм будівлі, зачистку кімнати, евакуацію пораненого з під обстрілу, дії в умовах вузького коридору або обмеженого огляду. Значною перевагою мобільних полігонів є їхня гнучкість у створенні тактичних сценаріїв, оскільки тренувальний простір може змінюватися після кожної серії вправ, що виключає ефект запам'ятовування маршруту і змушує стрільця адаптуватися до нової конфігурації середовища щоразу, як у реальному бою. Корисною також є інтеграція елементів динамічних мішеней, які несподівано з'являються в різних точках простору та імітують появу противника, що дозволяє перевірити не лише швидкість реакції, а й навички вибору моменту для пострілу та його обґрунтованість. У сучасних арміях використовуються також лазерні системи та пейнтбольні імітатори, що дають змогу проводити бойове злагодження підрозділів з мінімальним ризиком травм, але з високим рівнем реалізму тактичної взаємодії.

Другим аспектом підготовки стрільця до дій в обмеженому просторі є розвиток просторового мислення, що дозволяє швидко орієнтуватися у складних архітектурних умовах, виявляти потенційні зони укриття чи загрози та приймати оперативні рішення у стані динамічного навантаження. Просторове мислення, це не лише здатність візуалізувати планування приміщення чи оцінити відстань до цілі, але й уміння миттєво прорахувати вектор руху, знайти найближчу точку прикриття, адаптувати траєкторію пересування з урахуванням можливого вогню супротивника. Для розвитку цієї навички доцільним є включення в програму підготовки завдань на реконструкцію плану приміщення за коротким візуальним спостереженням, вправ з обмеженим часом на ухвалення рішення, а також моделювання критичних ситуацій, які вимагають зміни маршруту або позиції у відповідь на раптову загрозу [1].

Крім того, ефективне просторове мислення має бути доповнене вмінням миттєво оцінювати ступінь загрози, тобто диференціювати обстановку за ступенем ризику, визначати пріоритети ураження цілей, розрізняти супротивника та цивільних у стресовій ситуації. Такий сценарій передбачає далі не лише автоматизацію стрілецьких дій, а й формування внутрішньої моделі бойового рішення, коли стрілець діє не інстинктивно, а керуючись чіткими алгоритмами – наприклад, «оцінка → прицілювання → вогонь → перевірка оточення». Набуті навички доцільно формувати через застосування умовно несподіваних змін у сценарії, як, наприклад, поява «заручника» серед мішеней, або «неготової цілі», ураження якої вважається помилкою, що допоможе навчити стрільця не лише діяти, а й утримувати вогонь, коли це виправдано з точки зору обстановки, що є ознакою високої професійної зрілості.

Третім провідним фактором ефективного навчання є психологічна підготовка стрільця до бою в умовах ближнього контакту, що є однією з найбільш емоційно напружених форм бойової взаємодії. У ситуаціях, коли дистанція між противником і стрільцем не перевищує кількох метрів, коли рішення про відкриття вогню приймається у стані підвищеної тривоги, а обмежений простір позбавляє можливості для відступу чи маневру, на перший план виходять стресостійкість, самоконтроль, здатність діяти під психологічним тиском. Для досягнення цього стану в навчальному процесі слід імітувати бойові подразники – гучні звуки, раптові світлові спалахи, дим, вібрації, дії «ворога» або інструкторів, які непередбачувано втручаються в сценарій, що дає стрільцю можливість швидко адаптуватися до неспокійного середовища та зберігати концентрацію навіть у стані сенсорного перевантаження [8].

Крім того, специфічним компонентом психологічної підготовки є формування «бойового рефлексу», тобто здатності стрільця діяти автоматично, відповідно до алгоритмів поведінки, сформованих у процесі багаторазового повторення стандартних ситуацій. Практика бойових дій доводить, що саме ті військовослужбовці, які мають чітко відпрацьовані дії “до автоматизму”, демонструють найкращі результати під час реальних боїв. Тому програма підготовки повинна включати не лише тактичну стрільбу, а й елементи тактичного програмування поведінки, тобто формування послідовності дій на основі конкретної бойової ситуації: «вхід → огляд → пошук цілі → ураження → зміна позиції → перевірка тилу → доповідь» [14, 15]. Такого виду навчальне «програмування» має ефект у групових діях, де синхронізація рішень є запорукою безпеки.

Окремо маємо виділити факт того, що досягнення високого рівня бойової підготовки в умовах обмеженого простору є можливим лише за умови системного підходу до тренування, коли теоретичні знання, індивідуальні навички, групова взаємодія, психофізіологічна стійкість і технічна підготовленість розглядаються як взаємопов'язані елементи єдиної освітньо-тренувальної системи. Підрозділи, які регулярно залучаються до дій у складному урбанізованому середовищі, повинні проходити циклічні навчання, у рамках яких поетапно відпрацьовуються базові та складні сценарії, з поступовим ускладненням умов, зменшенням часу на реакцію, додаванням додаткових факторів ризику. Усі тренування мають супроводжуватися відеофіксацією та детальним розбором, що дозволяє виявляти тактичні помилки та формувати аналітичне мислення у стрільців.

Узагальнюючи дослідження зазначаємо, що ефективне застосування короткоствольної стрілецької зброї в умовах обмеженого простору є результатом не лише фізичної спроможності виконувати стрільбу в різних положеннях або тримати зброю під контролем, але й насамперед – глибокого розуміння тактичної логіки бою, чіткого дотримання алгоритмів входу в приміщення, бездоганного відпрацювання технік позиційної стрільби, а також постійного вдосконалення навичок командної роботи в стресових умовах.

Висновки. Аналіз застосування короткоствольної стрілецької зброї в умовах обмеженого простору показав, що її ефективність значною мірою визначається такими конструктивними й ергономічними характеристиками, як компактність, швидкість готовності до пострілу, зручність тримання та можливість точного ведення вогню однією рукою з нестандартних позицій. У таких ситуаціях особливе значення має адаптація зброї до специфіки внутрішнього архітектурного середовища: вузьких проходів, кімнат, сходових клітин, салонів транспортних засобів, де обмежено поле зору, ускладнено маневрування та знижено реакційну швидкість стрільця. У ближньому бою, коли дистанція до цілі не перевищує 10 метрів, традиційні моделі з довгою ствольною коробкою стають менш ефективними через свої габарити та складність швидкого використання. Короткоствольна зброя навпаки забезпечує оптимальні умови для оперативної реакції, завдяки чому є пріоритетним вибором у таких умовах. Важливими факторами успішного виконання бойового завдання є точність першого пострілу, час реакції на загрозу та здатність стрільця контролювати зброю в тісному просторі.

Особливості ближнього бойового контакту характеризуються високою швидкоплинністю подій, частими змінами позицій противника, обмеженими можливостями для укриття та неможливістю реалізації флангового маневру, що створює високі вимоги до психологічної стійкості, просторової орієнтації та вміння швидко приймати рішення. Водночас стрілець стикається з ризиками, пов'язаними з недостатнім оглядом, нестабільним положенням тіла, обмеженими можливостями для переміщення або відступу. Для підвищення ефективності використання короткоствольної зброї важливим є регулярне тренування в умовах, максимально наближених до реальних. Тактична підготовка має передбачати імітацію типових архітектурних обмежень, інтенсивне навантаження та акцент на інстинктивні дії, що забезпечує автоматизм у виконанні бойових прийомів. З цією метою рекомендовано використовувати комплексні тренувальні сценарії, такі як Double Tap, Mozambique Drill або Hostage Scenario, які моделюють високий ступінь непередбачуваності й вимагають миттєвої реакції.

Розроблено інтегровану методологію оцінки ефективності короткоствольної зброї в умовах ближнього бою, що базується на аналізі ключових параметрів: точність вогню, швидкість реакції на ціль, зручність управління, тактична безпека та стійкість до стресових факторів. Для систематичного розвитку навичок запропоновано багаторівневу систему тестування, від базових нормативів до складних бойових сценаріїв, що дає змогу точно диференціювати рівень бойової готовності. Значну роль у процесі підготовки відіграє тренувальна інфраструктура «kill house», макети приміщень, динамічні мішені, що сприяють формуванню автоматизованих навичок, адаптації до змін у середовищі, швидкому виявленню та нейтралізації загрози.

ЛІТЕРАТУРА:

1. Воробець Х.О. Використання новітніх методик під час викладання дисципліни «Вогнева підготовка» у вищих навчальних закладах зі специфічними умовами навчання. Підготовка поліцейських в умовах реформування системи МВС України : зб. наук. пр. МВС України, Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2019. 364 с. С. 316-318.
2. Гашенко С. В., Колдашов О. В., Брідня Є. О., Чалий М. Г. Особливості застосування стрілецької зброї збройними силами України. *Юридичний науковий електронний журнал*. 2024. № 5. С. 567–569. DOI: 10.32782/2524-0374/2024-5/141.
3. Задорожний К. А. Застосування стрілецької зброї підрозділами Національної гвардії України у протидії військовим загрозам. *Науковий вісник Київського інституту Національної гвардії України*. 2024. № 1. С. 61–67. DOI: 10.59226/2786-6920.1.2024.61-67.
4. Мельник І. М., Канюка В. Є., Богайчук В. І. Основи володіння зброєю та вогневої підготовки студентів спеціальності «Правоохоронна діяльність» з використанням елементів снайпінгу. *Наукові записки. Серія: Право*. 2023. № 14. С. 183-186. DOI: <https://doi.org/10.36550/2522-9230-2023-14-183-186>
5. Міністерство оборони України, Апарат Головнокомандувача Збройних Сил України. Генеральний штаб Збройних Сил України. Центр досліджень воєнної історії Збройних Сил України. Зброя російсько-української війни 2022 – 2023 років : довідник-каталог основних зразків озброєння та військової техніки, які застосовувалися противорчними сторонами під час відсічі широкомасштабного вторгнення РФ в Україну (24.02.2022 – 30.06.2023) / Міністерство оборони України, Апарат Головнокомандувача ЗС України, Генеральний штаб ЗС України, Центр досліджень воєнної історії ЗС України. Київ : Видавництво Ліра-К, 2023. 243 с.
6. Шовкун В. М. Зв'язок між рівнем вогневої підготовки українських військових підрозділів та ефективністю їхніх бойових дій. *Академічні візії*. 2024. № 36. DOI: 10.5281/zenodo.13908774.
7. Явтушенко В. О., Корчагін М. В., Козлов Д. М., Мороховський М. Л., Коплік О. М., Холодняк М. Ю. Вплив фізичної, психологічної та тактичної підготовки стрільця на ефективність стрільби зі стрілецької зброї. *Scientific Collection «InterConf+»*. 2023. № 39 (179). С. 580–595. DOI: 10.51582/interconf.19-20.11.2023.060.
8. Ясько В.А., Ментус І.Е., Бамбуляк М.П., Кучинський С.А. Стрілецька зброя та вогнева підготовка. Частина 1. Основи стрільби зі стрілецької зброї. Кам'янець-Подільський: КІНУ, 2022. 164 с.
9. Danielsson A. G. S. The Emergence of a Military Urban in and of War. *Annals of the American Association of Geographers*. 2025. Vol. 115, No 2. p. 404–418. DOI: 10.1080/24694452.2024.2422856
10. Gage T. Active Shooter Trainings: An Effectiveness Study. Thesis for Master of Science in Psychology, University of Louisiana at Lafayette. 2024. June. DOI: 10.13140/RG.2.2.31071.06567.
11. Greenlee J. G. S. The Tradition of Short-Barreled Rifle Use and Regulation in America. SSRN. 2025. Posted January 12, 2025. e-print, 28 p. DOI: 10.2139/ssrn.5094701.
12. Maitre M., Chiaravalle A., Horder M., Chadwick S., Beavis A. Evaluating the effect of barrel length on pellet distribution patterns of sawn-off shotguns. *Forensic Science International*. 2021. Vol. 320, Article 110685. DOI: 10.1016/j.forsciint.2021.110685
13. Muženič M. Handling Weapons as a Source of Security Threats in the Local Environment. *Danube*. 2023. № 14 (1). p. 26–44. DOI: 10.2478/danb-2023-0002.
14. Olma J., Sutter C., Sülzenbrück S. Blended police firearms training improves performance in shoot/don't shoot scenarios: a systematic replication with police cadets. *Frontiers in Psychology*. 2024. Volume 15. S. (e-article 1495812). DOI: 10.3389/fpsyg.2024.1495812.
15. Žnidaršič V., Petrovski A., Radovanović M. Characteristics of contemporary combat operations in urban areas. *Proceedings of the 9th International Scientific Conference GEOBALCANICA 2023*. 2023. May. Vol. 149. p. 149–158. DOI: 10.18509/GBP23149zh.

REFERENCES:

1. Vorobets K. O. (2019), "Vykorystannia novitnikh metodyk pid chas vykladannia dystsypliny 'Voieva pidhotovka' u vyshchyykh navchalnykh zakladakh zi spetsyfichnymy umovamy navchannia" [Using innovative methods in teaching the subject "Fire training" in higher educational institutions with specific training conditions], *Pidhotovka politseiskykh v umovakh reformuvannia systemy MVS Ukrainy: zbirnyk naukovykh*

prats MVS Ukrainy, Kharkivskiy natsionalnyi universytet vnutrishnikh sprav, Kharkiv: KhNUVS, 364, pp. 316–318.

2. Hashenko S. V., Koldashov O. V., Bridnia Ye. O., Chalyi M. H. (2024), “Osoblyvosti zastosuvannya striletskoi zbroi Zbroinykh Syl Ukrainy” [Peculiarities of using firearms by the Armed Forces of Ukraine], *Yurydychni naukovyi elektronnyi zhurnal*, No. 5, pp. 567–569. DOI: 10.32782/2524-0374/2024-5/141.

3. Zadorozhnyi K. A. (2024), “Zastosuvannya striletskoi zbroi pidrozdilamy Natsionalnoi hvardii Ukrainy u protydii viiskovym zahrozam” [Use of firearms by National Guard units of Ukraine in countering military threats], *Naukovi visnyk Kyivskoho instytutu Natsionalnoi hvardii Ukrainy*, No. 1, pp. 61–67. DOI: 10.59226/2786-6920.1.2024.61-67.

4. Melnyk I. M., Kaniuka V. Ye., Bohaichuk V. I. (2023), “Osnovy volodinnia zbroieiu ta vohnevoyi pidhotovky studentiv spetsialnosti ‘Pravookhoronna diialnist’ z vykorystanniam elementiv snaipinhu” [Fundamentals of weapon handling and fire training for law enforcement students using elements of sniping], *Naukovi zapysky. Seriya: Pravo*, No. 14, pp. 183–186. DOI: <https://doi.org/10.36550/2522-9230-2023-14-183-186>.

5. Ministerstvo oborony Ukrainy, Aparat Holovnokomanduvacha ZSU, Heneralnyi shtab ZSU, Tsentr doslidzhen voiennoi istorii ZSU. (2023), *Zbroia rosiisko-ukrainskoi viiny 2022–2023 rokiv: dovidnyk-katalog osnovnykh zrazkiv ozbroiennia ta viiskovoi tekhniki* [Weapons of the Russian-Ukrainian war of 2022–2023: handbook-catalog of main weapon and military equipment types], Kyiv: Vydavnytstvo Lira K, 243 p.

6. Shovkun V. M. (2024), “Zviazok mizh rivnem vohnevoyi pidhotovky ukrainskykh viiskovykh pidrozdiliv ta efektyvnistiu yikhnikh boiovykh dii” [The connection between the level of fire training of Ukrainian military units and the effectiveness of their combat actions], *Akademichni vizii*, No. 36. DOI: 10.5281/zenodo.13908774.

7. Yavtushenko V. O., Korchahin M. V., Kozlov D. M., Morokhovskiy M. L., Koplik O. M., Kholodniak M. Yu. (2023), “Vplyv fizychnoi, psykholohichnoi ta taktychnoi pidhotovky striltsia na efektyvnist strilby zi striletskoi zbroi” [Impact of physical, psychological, and tactical training of shooters on the effectiveness of firearm shooting], *Scientific Collection «InterConf+»*, No. 39(179), pp. 580–595. DOI: 10.51582/interconf.19-20.11.2023.060.

8. Yasko V. A., Mentus I. Ye., Bambuliak M. P., Kuchynskiy S. A. (2022), *Striletska zbroia ta vohneva pidhotovka. Chastyna 1. Osnovy strilby zi striletskoi zbroi* [Firearms and fire training. Part 1. Fundamentals of shooting from firearms], Kamianets-Podilskiy: KPNPU, 164 p.

9. Danielsson A. G. S. (2025), “The Emergence of a Military Urban in and of War”, *Annals of the American Association of Geographers*, Vol. 115, No. 2, pp. 404–418. DOI: 10.1080/24694452.2024.2422856.

10. Gage T. (2024), *Active Shooter Trainings: An Effectiveness Study*, Thesis for Master of Science in Psychology, University of Louisiana at Lafayette. June. DOI: 10.13140/RG.2.2.31071.06567.

11. Greenlee J. G. S. (2025), “The Tradition of Short Barreled Rifle Use and Regulation in America”, SSRN, e-print, 28 p. Posted January 12, 2025. DOI: 10.2139/ssrn.5094701.

12. Maitre M., Chiaravalle A., Horder M., Chadwick S., Beavis A. (2021), “Evaluating the effect of barrel length on pellet distribution patterns of sawn off shotguns”, *Forensic Science International*, Vol. 320, Article 110685. DOI: 10.1016/j.forsciint.2021.110685.

13. Muženič M. (2023), “Handling Weapons as a Source of Security Threats in the Local Environment”, *Danube*, No. 14(1), pp. 26–44. DOI: 10.2478/danb-2023-0002.

14. Olma J., Sutter C., Sülzenbrück S. (2024), “Blended police firearms training improves performance in shoot/don’t shoot scenarios: a systematic replication with police cadets”, *Frontiers in Psychology*, Vol. 15, e-article 1495812. DOI: 10.3389/fpsyg.2024.1495812.

15. Žnidaršič V., Petrovski A., Radovanović M. (2023), “Characteristics of contemporary combat operations in urban areas”, *Proceedings of the 9th International Scientific Conference GEOBALCANICA 2023*, May, Vol. 149, pp. 149–158. DOI: 10.18509/GBP23149zh.

TACTICAL FEATURES OF USING SHORT-BARRELED FIREARMS IN CONFINED SPACES

The article is dedicated to the study of tactical features of using short-barreled firearms in confined spaces, particularly in urban environments where key factors include response speed, maneuverability, and coordination of actions. The research analyzes the specifics of close-quarters combat, emphasizing the necessity of adapting firearms training to the conditions of tight indoor spaces. The aim of the article is to substantiate methodological foundations for the effective use of short-barreled firearms in restricted environments, to develop criteria for assessing their combat effectiveness, and to propose recommendations for improving tactical training programs for personnel. The study employs analysis of literature sources on close-combat tactics, technical characteristics of firearms, and shooting training methodologies, as well as empirical data obtained through modeling combat scenarios in training modules such as “kill houses.” The research involved weapon testing for accuracy, reaction speed, ergonomics, and safety in specially designed environments simulating real combat situations. It has been established that short-barreled firearms, particularly pistols, provide high efficiency in close combat due to their compactness, quick readiness, and the ability to fire from unconventional positions—factors that are critically important in confined areas. A comprehensive evaluation system is proposed, encompassing accuracy, speed, ergonomics, tactical safety, and the shooter’s psychophysiological resilience, allowing for objective determination of combat capability. The scientific novelty lies in the formalization of tactical algorithms for both individual and group actions, as well as in the development of exercises that consider the specifics of restricted spaces, including positional shooting and room-entry techniques. The results highlight the importance of integrating psychophysiological preparation and stress modeling to improve shooter performance. Future research may focus on integrating virtual and augmented reality technologies to create realistic training simulators that replicate combat conditions. Promising directions also include the study of modern aiming systems and auxiliary equipment to enhance shooting accuracy and speed in confined environments.

Keywords: short-barreled firearms, close combat, confined space, tactical training, performance evaluation, firearms training.

ЦИФРОВІ ТЕХНОЛОГІЇ В ФОРМУВАННІ МЕТОДИКИ ОЦІНЮВАННЯ БОЙОВОЇ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ КОРОТКОСТВОЛЬНОЇ СТРІЛЕЦЬКОЇ ЗБРОЇ

Стаття присвячена дослідженню цифрових технологій для оцінювання бойової ефективності короткоствольної стрілецької зброї в реальних і симульованих бойових умовах. Вона аналізує еволюцію віртуальних стрілецьких тренажерів та їхню роль у підвищенні точності аналізу стрільби й тактичної підготовки. Метою дослідження є встановлення рівня ефективності використання цифрових систем для забезпечення об'єктивного оцінювання технічних параметрів зброї та вдосконалення тактичних підходів до її бойового застосування. Для аналізу використано систематичний огляд сучасних систем віртуального тренування, включаючи оптико-електронні сенсори, лазерні імітатори, інфрачервоні трекінгові технології та AR/VR-системи. Методологія базується на порівняльному аналізі функціональних можливостей систем, їхньої здатності фіксувати параметри стрільби (траєкторія ствола, стабільність, час реакції) та обробляти дані за допомогою спеціалізованого програмного забезпечення. Результати дослідження демонструють, що цифрові технології забезпечують високоточну реєстрацію ключових параметрів стрільби, таких як: відхилення ствола, момент натискання на спусковий гачок і розсіювання, що дозволяє виявляти конструктивні недоліки зброї. Системи також дають змогу моделювати динамічні бойові сценарії, включаючи урбанізоване середовище та стресові умови, забезпечуючи комплексний аналіз індивідуальних і групових тактичних дій. Наукова новизна полягає в інтеграції сенсорних платформ, ігрових рушіїв та біометричних даних (частота серцевих скорочень, рівень стресу) для створення цифрового профілю бойової ефективності, що враховує як технічні, так і фізіологічні аспекти. Запропонований підхід відкриває нові можливості для об'єктивного порівняння різних моделей зброї та їхньої адаптації до сучасних бойових доктрин. Перспективи подальших досліджень включають розробку систем із підтримкою симуляції для підвищення рівня занурення в симульоване середовище. Розвиток може отримати уніфікована цифрова модель оцінювання, яка інтегруватиме дані про індивідуальну та групову тактичну взаємодію для формування комплексних бойових профілів.

Ключові слова: короткоствольна зброя, бойова ефективність, цифрові технології, стрілецька підготовка, віртуальні тренажери, сенсорні системи, тактика застосування, тактичне моделювання.

Вступ та постановка проблеми. У сучасних умовах радикального ускладнення глобальної військово-стратегічної ситуації, що характеризується зростанням кількості регіональних збройних конфліктів, розширенням зон бойових дій та зміною характеру воєнного протистояння, особливого значення набуває питання точного, оперативного та об'єктивного оцінювання бойової ефективності озброєння, зокрема короткоствольної стрілецької зброї, яка часто використовується у ближньому бою, штурмових операціях, антитерористичних місіях та бойових діях в стиснених умовах. Зважаючи на трансформацію сучасної тактики збройної боротьби, яка дедалі більше орієнтується на мобільність, швидкість реагування, мінімізацію логістичних затрат і максимально ефективного використання особистої стрілецької зброї, виникає об'єктивна потреба у створенні таких технологічних рішень, які дозволяють оперативно вимірювати, аналізувати та порівнювати бойову результативність короткоствольних зразків в умовах реального застосування. У цих умовах традиційні методи оцінки, що базуються переважно на статистичних спостереженнях або суб'єктивних висновках польових командирів, виявляються недостатніми для комплексного врахування численних факторів, що впливають на бойову ефективність зброї.

Цифрові технології, які охоплюють сенсорні системи, алгоритми обробки великих масивів даних, моделювання динаміки стрільби, машинне навчання, відеоаналітику та мобільні платформи збору даних, відкривають нові можливості для всебічного аналізу функціонування короткоствольної стрілецької зброї у бойовій ситуації. Впровадження таких технологій дозволяє не лише здійснювати комплексне оцінювання точності, швидкості, надійності та стійкості зразків, а й виявляти їхні переваги та недоліки залежно від специфіки театру бойових дій, типу операцій та умов середовища. Отже, актуальність дослідження зумовлена нагальною потребою у впровадженні цифрових підходів до оцінювання бойових характеристик короткоствольної зброї, що дає змогу не лише оптимізувати процеси збройного забезпечення, але й посилити ефективність її застосування на сучасному полі бою, де кожен технічний параметр може мати критичне значення для успіху оперативної місії.

Аналіз основних наукових досліджень і публікацій. Аналіз наукових джерел з питань оцінки бойової ефективності короткоствольної зброї за допомогою цифрових технологій показує, що фахівці в Україні та за кордоном активно досліджують технічні та тактичні аспекти стрілецької підготовки. Сучасні військові реалії вимагають нових підходів до тренувань, і груп дослідників [1-12] доводять ефективність цифрових тренажерів для покращення точності стрільби в обмежених просторах. Окремі проблемні питання використання віртуальних тренувальних систем розглядають фахівці [3], [7], які показують, що технології ефективно розвивають не лише індивідуальні навички, а й вміння діяти у складі підрозділу. Дослідження [5], [10] доповнюють цю картину, демонструючи, як інфрачервоні датчики та біометричні системи допомагають оцінювати готовність бійців до реальних бойових умов.

Проте наука ще не дала відповіді на низку ключових питань. Наприклад, досі недостатньо вивчено, як саме рухається ствол під час пострілу в умовах стресу або обмеженої видимості. Також залишається відкритим питання про об'єднання даних з різних датчиків – відео, звуку, тактильних сигналів – в єдину систему аналітики. Крім того, більшість сучасних досліджень зосереджені на індивідуальних показниках стрільця, тоді як реальні бойові умови вимагають розуміння групової взаємодії, особливо в міському середовищі. Ці прогалини в наукових знаннях свідчать про те, що на сьогодні як ніколи потрібні нові дослідження. Вони мають допомогти створити комплексну методику оцінки ефективності короткоствольної зброї, яка враховуватиме не лише технічні характеристики, а й поведінку стрільця в складних умовах реального бою.

Метою статті є: проведення дослідження ефективності використання цифрових систем для забезпечення оцінювання технічних параметрів стрілецької зброї та вдосконаленні тактичних підходів до її бойового застосування.

Виклад основного матеріалу. У бойовій практиці ефективність використання короткоствольної зброї визначається сукупністю параметрів, які складно зафіксувати в реальному часі за допомогою класичних методів спостереження чи документування. Серед таких параметрів варто виокремити стабільність зброї під час ведення вогню, точність та розсіювання пробойн, темп стрільби, швидкість прицілювання, а також здатність зброї зберігати працездатність у стресових умовах та при фізичних перевантаженнях, пилу, вологи, обмеженому освітленні тощо. Водночас навіть у польових умовах існує можливість використовувати новітні цифрові технології, які дозволяють об'єктивно, автоматизовано і з високим рівнем достовірності здійснювати збір та аналіз даних щодо бойової ефективності стрілецької зброї.

Одним з перспективних напрямів є впровадження оптико-електронних та інтерактивних систем фіксації стрільби, які базуються на сенсорному контролі переміщення зброї та автоматизованій реєстрації результатів ураження [2]. Ці системи включають в себе електронні пристрої, що закріплюються на зброї або імітують її конструкцію, і дають змогу у реальному часі відслідковувати траєкторію ствола, момент натискання на спусковий гачок, фазу прицілювання та інші ключові параметри стрільби. Завдяки синхронізації з комп'ютерним програмним забезпеченням, дані передаються на дисплей, де з високою точністю

візуалізуються дії стрільця, що дозволяє здійснювати об'єктивне оцінювання кожного пострілу (рис. 1).

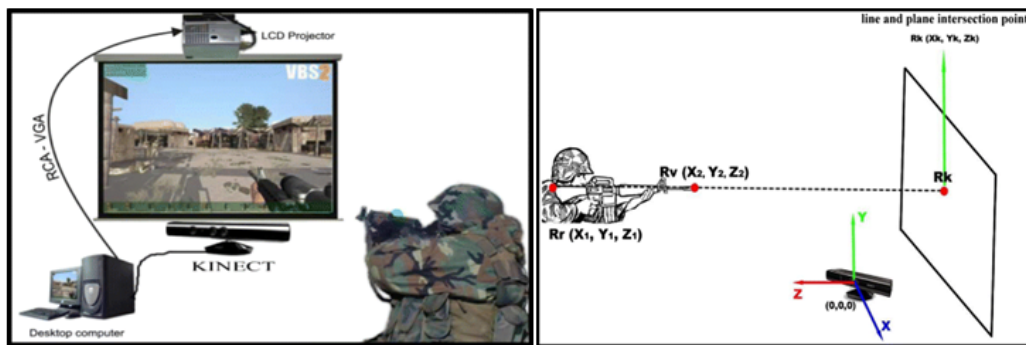


Рисунок 1 - Стационарна система електронного контролю застосування стрілецької зброї [11]

У бойових умовах, коли використання бойових набоїв не завжди дозволяє точно визначити помилки стрільця через ефект віддачі або динамічність ситуації, саме цифрові системи надають можливість з високою деталізацією фіксувати миттєві відхилення зброї від осі прицілювання, затримки у натисканні на спусковий гачок або некоректну лінію ведення ствола. Це, своєю чергою, дає змогу виявляти системні недоліки в конструкції конкретної моделі зброї, а також коригувати тактичні підходи до її застосування в тій чи іншій обстановці.

Крім того, електронні стрілецькі тренажери й бойові тири з цифровими сенсорними системами широко застосовуються для імітаційної апробації короткоствольної зброї в умовах, що максимально наближені до реальних бойових дій (рис. 2).

Іншим фактором цифрового аналізу є можливість довготривалого зберігання, структурування та порівняння результатів стрільби з різних зразків короткоствольної зброї, що забезпечує формування об'єктивної бази даних для подальших технічних удосконалень. Зокрема, сучасні цифрові системи можуть генерувати аналітичні звіти щодо середнього часу реакції стрільця, кількості влучань, зниження точності при підвищенні темпу стрільби тощо. Така інформація є вкрай цінною не лише для безпосереднього оцінювання вже існуючих зразків зброї, а й для формування технічного завдання на нові моделі, які мають відповідати сучасним вимогам до бойової ефективності.



Рисунок 2 - Цифрова імітація стрільби з короткоствольної стрілецької зброї в умовах віртуального тиру з оцінюванням бойової ефективності

У сучасній реальності, коли бойові дії за своєю природою стали швидкоплинними, багатофакторними й часто відбуваються в умовах обмеженого простору і зосередитися на розвитку методів, які дозволяють точно та оперативно оцінювати бойову ефективність короткоствольної стрілецької зброї, що стала ключовим елементом ближнього бою, штурмових операцій і бойових дій в урбанізованому середовищі, де швидкість реагування, точність пострілу та здатність пристосовуватися до непередбачених змін обстановки можуть визначати результат тактичних зіткнень. При цьому традиційні підходи до фіксації результатів бойового застосування, що базуються на спостереженнях командира або аналізі статистики влучень, не здатні забезпечити належної точності й глибини оцінювання, особливо коли йдеться про такі суто технічні параметри, як траєкторія руху ствола під час натискання на спусковий гачок, момент виникнення пострілової хвилі, швидкість прицілювання, стабільність зброї при веденні серійної стрільби в умовах руху або обмеженого простору.

Відтак, інтеграція цифрових технологій у процес моніторингу та аналізу бойового використання стрілецької зброї стає не просто доцільною, але й критично важливою: саме за допомогою сенсорних платформ, відеоаналітики, алгоритмів обробки великих масивів даних і цифрового моделювання відкривається можливість у режимі реального часу отримувати об'єктивну інформацію про ефективність кожного пострілу, а також виявляти системні недоліки зброї чи тактики застосування у заданому типі бойового середовища [6]. Показані системи, зокрема оптико-електронні сенсори, лазерні імітатори, інтерактивні бойові тири, спеціальні пристрої сухого вогню (dry-fire), дозволяють закріплювати на зброї датчики, здатні з високою точністю фіксувати рух ствола від початку прицілювання до моменту натискання на тригер, одночасно забезпечуючи реєстрацію координат попадання або відхилення щодо цілі. Ці дані передаються в цифровій формі до комп'ютерної системи, де спеціалізоване програмне забезпечення аналізує траєкторії, час реакції, точність, розсіювання патронів або імітованих пострілів, швидкість переходів між цілями та загальну стійкість зразка зброї під навантаженнями (рис. 3).

У бойових умовах, де використання бойових набоїв може бути обмеженим через фактори логістики або безпеки, саме цифрові рішення надають перевагу: оскільки ефект віддачі часто ускладнює аналіз механіки пострілу, застосування сухого вогню з реєстрацією лазерного імпульсу або руху ствола дає змогу оцінювати техніку стрільби з міліметровою точністю, виявляти відмінності між двома послідовними пострілами навіть при «пуля в пулю», розрізняти промахи, локалізувати точку попадання й аналізувати вплив фізичних умов (наприклад, рух стрільця, нестабільне положення, обмежений час) на якість стрільби.



Рисунок 3 – Віртуальна симуляція бойового застосування стрілецької зброї у тири з використанням цифрової імітації бою [14]

Наступним елементом є цифрова архівація та аналітика: всі дані щодо стрільби можуть бути збережені для подальшого порівняльного аналізу різних моделей короткоствольної

стрілецької зброї, різних конфігурацій (оптичні приціли, глушники, рукоятки), а також в різних типах бойових умов — це створює інформаційну базу, на якій можна формувати технічні вимоги до нових конструкцій зброї або обирати оптимальне оснащення підрозділів для певного типу операцій. Одна з систем, яка може бути використана для оцінки бойової ефективності короткоствольної стрілецької зброї в цифровому контексті, це MantisX, революційна платформа, яка підключається до стандартної короткоствольної зброї (пістолета чи револьвера), кріпиться на рейку аксесуарів, з'єднується з мобільним додатком і здатна фіксувати найменший рух у момент струсу зброї під час пострілу або імітованого dry-fire за допомогою лазерних капсулок або живих патронів, при цьому генеруються дані про рух зброї під час натискання курка, відхилення, швидкість підняття прицілу та інші (рис. 4) [8].



Рисунок 4 - Цифрова система MantisX для оцінювання бойової ефективності короткоствольної стрілецької зброї за допомогою мобільного додатку [8]

Платформа MantisX дозволяє миттєво отримати зворотний зв'язок у вигляді графічного та числового аналізу кожного пострілу, визначає технічні помилки, дає рекомендації щодо покращення техніки володіння зброєю і усе це в реальному часі й без використання боєприпасів. Система MantisX показує приклад того, як цифрові технології можуть бути використані напряду в бойових умовах для оцінювання бойової ефективності: аналіз стабільності зброї під час пострілу, точності прицілювання, часу реакції, а також відстеження динаміки руху зброї в момент, коли бій ведеться в обмеженому просторі, під стресом або в умовах низької видимості. Зокрема, сучасні віртуальні стрілецькі тренажери (Virtual Small Arms Trainer – VSAT) вже давно вийшли за межі суто навчальної функції, перетворившись на повноцінні цифрові системи тактичної імітації, здатні імітувати динамічні бойові сценарії, аналізувати дії стрільця в режимі реального часу й формувати комплексну картину ефективності використання зброї на полі бою.

Традиційно вся система стрілецької підготовки, що включала й оцінювання характеристик зброї, стикалася з низкою суттєвих викликів: надмірна вартість реального стрільбища, постійні витрати на боєприпаси, амортизація зброї та спорядження, а також екологічне навантаження і зокрема шумове та повітряне забруднення внаслідок стрільби бойовими патронами. Усе це створювало перешкоди для регулярного аналізу ефективності зброї в бойовій ситуації, оскільки реальні умови часто виявлялися непередбачуваними, а точна фіксація поведінки зброї та користувача в обмеженому часовому проміжку і об'єктивно неможливою. До того ж, класичні умови стрільби як-от погодні коливання, відсутність контролю над фоновими умовами, складність відтворення ідентичних ситуацій — ставали обмеженням для точного й повторюваного оцінювання. Сама ж динаміка бойової обстановки, що включає змінну видимість, психологічний тиск, необхідність швидкого прицілювання, використання зброї в русі або з нестандартного положення, вкрай складно відтворюється у звичайному тирі. Водночас цифрові технології дозволяють подолати цей бар'єр, створюючи повністю контрольоване і водночас реалістичне середовище [9].

Зі стрімким розвитком комп'ютерної графіки у 1980-х роках почали з'являтися перші прототипи VSAT-систем, які за своєю суттю імітували електронні галереї та стрілецькі рубежі. Першочергово їх призначенням було створення моделі переходу від ручної техніки володіння зброєю до фактичного бойового застосування, де можна було відпрацювати як розміщення зброї, так і командні сигнали, черговість цілей тощо. Вони дозволяли імітувати стрільбу з різних положень, тренувати дихальні цикли, стабілізувати рух зброї під час прицілювання, а також вивчати такі нюанси, як зведення та «ведення» рухомої цілі, або вплив нахилу зброї на траєкторію кулі. Важливо, що такі пристрої з самого початку почали використовувати цифрові датчики, які могли фіксувати неточності стрільця і повторювати ідентичний сценарій для перевірки динаміки змін. Попри очевидні переваги, ранні покоління VSAT не вирішували ключового завдання через інтеграцію цілої бойової групи в симульоване бойове середовище, де потрібно не лише стріляти, а й комунікувати, приймати рішення, координувати застосування різних видів зброї. Саме для цього було створено більш потужні, адаптивні й модульні комплекси нового покоління, які дозволяють оцінювати ефективність не окремого пострілу, а повного комплексу дій у рамках тактичного епізоду.

Зокрема система Ground Combat Indoor Trainer (GCIT) від компанії Saab стала прикладом такого підходу. Вона надає можливість одночасно тренувати індивідуальну стрільбу з короткоствольної або автоматичної зброї, а також відпрацьовувати дії підрозділу проти статичних чи динамічних цілей. Така система дозволяє фіксувати помилки у реальному часі, аналізувати поведінку зброї на кожному етапі — від прицілювання до пострілу і точно розраховувати ефективність ведення вогню в симульованих бойових обставинах.

Серед інших відомих рішень це Guardiaris SATT (Small Arms Tactical Trainer), який дозволяє проводити оцінку стрільби в урбанізованому середовищі з багатьма учасниками одночасно, та Thales SATIS, де підтримується великий арсенал типів зброї, включаючи навіть міномети, що дозволяє змодельовати комплексне поле бою. Суттєвою перевагою VSAT-платформ нового покоління є їхня модульність, а саме можливість оновлення апаратного та програмного забезпечення, інтеграція нових видів зброї або оновлення існуючих сценаріїв відповідно до змін у бойових доктринах. Віртуальні системи оцінювання, побудовані на основі цифрових технологій, дозволяють створити нову якість аналізу, коли ключові параметри, такі як точність, швидкість реагування, стабільність зброї, рухливість у просторі та фіксуються в цифровому форматі, зберігаються, порівнюються та використовуються для формування повноцінного профілю бойового застосування конкретної моделі зброї або її комбінацій з аксесуарами [7].

Однією з найяскравіших ілюстрацій цієї технологічної трансформації є приклад Корпусу морської піхоти США, який реалізував проект Indoor Simulated Marksmanship Trainer (ISMT). Поточна версія – ISMT III вже була модернізована для того, щоб забезпечити можливість цифрового відтворення вогневих дій з використанням не лише короткоствольної зброї, а й мінометів калібру 81 мм. Розроблена компанією InVeris Training Solutions (раніше FATS, потім Meggitt), система ISMT дає змогу здійснювати бойове моделювання у будь-який час, без обмежень, пов'язаних із погодою, наявністю стрільбища або ризиками, притаманними реальним бойовим умовам. Саме така віртуалізація дозволяє досягти максимальної оперативної готовності та оцінювати дії стрільця або команди у сценаріях, максимально наближених до реального бою.

Подібну логіку запозичили і європейські країни. Так, Австрійська армія впровадила передову систему Guardiaris SATT, яка встановлена у Брукнойдорфі, а згодом ще у п'яти місцях. Кожен з таких комплексів включає параболический екран з горизонтальним полем зору 148°, чотири проектори для створення панорамного зображення, систему об'ємного звуку з чотирма динаміками, вібраційну підлогу та центральну станцію керування (Instructor Operator Station – IOS). Саме через IOS інструктор має можливість формувати бойовий сценарій, запускати його, відстежувати дії кожного учасника та здійснювати детальний розбір дій після завершення епізоду. Візуальна система SATT створена на ігровому рушії, що дає змогу моделювати зміну доби, погодних умов, нічне бачення (NVG) та інші параметри бойового

середовища. Унікальність цієї системи полягає в тому, що вона не використовує лазерні імпульси, а застосовує власну інфрачервону (IR) технологію трекінгу для надточного фіксування позицій стрільця та орієнтації зброї [12]. З останніх оновлень – це інтеграція протитанкових систем ближньої дії, а також режимів снайперської стрільби на дистанції. У рамках європейського проекту FIIST (Future Integrated Indoor Soldier Training), підтриманого Європейською програмою розвитку оборонної промисловості, компанія Guardiaris спільно з ITEC GmbH, Madritsch і Instalaza розробляє також підтримку дистанційно керованих вогневих модулів (Remote Weapon System – RWS), що може значно розширити можливості тактичного моделювання в цифрових середовищах.

Окрему увагу збройні сили приділяють впровадженню біометричних і комунікаційних показників як складових цифрового профілю. Йдеться про моніторинг частоти серцевих скорочень, рівня стресу, потовиділення, розпізнавання голосових та жестових команд, що в сукупності дозволяє не лише аналізувати дії стрільця, а й розуміти його бойову стійкість у складних умовах. У перспективі такі дані будуть акумулюватися у формі цифрового дос'є на кожного військовослужбовця або підрозділ, що дозволить приймати точні рішення про доцільність використання певного типу зброї в тій чи іншій обстановці [3].

Одним із головних викликів для військових у цьому контексті залишається складність реалістичного відтворення бойового середовища під час стрільб із реальних стрільбищ. Як правило, такі майданчики побудовані лінійно, цілі розташовані фронтально — що повністю суперечить умовам реального бою. У віртуальному середовищі ці обмеження зникають, однак технологічно VSAT-системи довгий час змушені були імітувати ті ж лінійні рубежі. Для подолання цього обмеження компанія InVeris Training Solutions розробила AR/VR-системи – SRCE та SURVIVR, що створюють повноцінне 360-градусне віртуальне середовище, де військовослужбовець, одягнувши шолом з високою роздільною здатністю, перебуває у змодельованому світі з накладеними об'єктами: перешкодами, вогневими точками, противником, союзниками та цивільними особами [13]. Таке середовище забезпечує зорові й звукові сигнали, дозволяє генерувати сценарії з багатьма змінними та відслідковувати ефективність дій стрільця при різних параметрах бою (рис. 5).



Рисунок 5 - Віртуальне стрілецьке тренування з використанням рішень VR/AR від InVeris Training Solutions [13]

Одним із ключових напрямів сучасного військового інноваційного середовища, що стосується оцінювання ефективності використання короткоствольної стрілецької зброї в реальних бойових умовах, є активне впровадження цифрових технологій у сферу віртуального моделювання, зокрема через розширення можливостей так званих VSAT-систем (Virtual Small Arms Trainer). Центральною метою використання цих систем у бойовому контексті є не лише імітація стрілецької взаємодії, а й повноцінна аналітика, що дозволяє фіксувати,

систематизувати й порівнювати ефективність зброї в динамічному, змодельованому середовищі, максимально наближеному до бойового простору.

Досягнення відчуття повного занурення в бойову ситуацію, тобто створення ефекту «призупинення недовіри» є одним з фундаментальних критеріїв ефективності таких симуляцій. Для цього система повинна стимулювати якомога більше сенсорних каналів, насамперед зоровий, який є головним для орієнтації людини в просторі. Саме тому останні покоління візуальних VSAT-платформ активно переходять на рушії візуалізації ігрового рівня, такі як VBS4 (Virtual Battlespace 4) від Bohemia Interactive або Unreal Engine 5 від Epic Games [11].

У США, зокрема, компанія Laser Shot вже тривалий час застосовує рушій VBS у своїх продуктах, що дозволяє створювати реалістичні сценарії бойового застосування короткоствольної зброї. У 2023 році компанія VirTra оголосила про успішну інтеграцію VBS4 у власну операційну систему VOS, що стало важливим кроком до спроможності ще глибшого занурення тих хто навчається у реалістичний бойовий простір - ціленаправленна підготовка. Основною перевагою такого підходу є можливість створення геоприв'язаних віртуальних середовищ, які точно відтворюють реальні стрільбища, локації ведення бойових дій або навіть конкретні ділянки місцевості для проведення місій, що своєю чергою відкриває шлях до точного оцінювання результативності застосування стрілецької зброї в заданому бойовому контексті. До недавнього часу військові були змушені використовувати окремі CGI-модулі для різних тренажерних систем, кожна з яких мала власні бази даних та вимагала високих ресурсів для підтримки. Сучасні ігрові рушії дозволяють уніфікувати ці ресурси: зокрема, інтеграція VBS4 надає змогу миттєво використовувати існуючі 3D-моделі зброї, рельєфів місцевості, бойових сценаріїв, що значно підвищує точність бойового моделювання. Наприклад, компанія Thales, яка створила лінійку VSAT-рішень під назвою Small Arms Training Indoor Simulator, перейшла на використання графічного рушія Unreal Engine 5, що дозволяє не лише відтворювати реалістичні візуальні ефекти, а й забезпечує високоточну візуалізацію траєкторій куль, взаємодії з перешкодами, ефектів диму, пилу, відблисків, блискавичних спалахів і усе це наближає симуляцію до справжнього поля бою (рис. 6).



Рисунок 6 - Симулятор стрілецької підготовки в приміщенні (VSAT) від Thales з використанням графічного рушія Unreal Engine 5 [13]

Хоча основна увага зосереджена на зоровому сприйнятті, одним із перспективних напрямів занурення є стимуляція нюху, це компонент, що досі залишається майже поза увагою розробників. Єдиним помітним прикладом була демонстрація компанії Cubic Defense, яка впровадила симуляцію запахів у віртуальному тренажері, зокрема для відтворення специфічного аромату афганського села. Враховуючи значення нюху у реальному бойовому досвіді, подальший розвиток цієї технології видається доцільним з огляду на глибину занурення в модельовану обстановку.

Новітній тренд також включає розвиток доповненої (AR) та віртуальної реальності (VR), зокрема через продукти компанії InVeris, такі як SRCE та SURVIVR, які забезпечують 360-градусне бойове середовище. Стрілець одягає гарнітуру з високою роздільною здатністю, яка не лише передає візуальні та звукові сигнали, а й доповнює реальний світ накладеними об'єктами, такими як вороги, цивільні, укриття або пересувні перешкоди, що імітують справжнє бойове середовище у його повній складності. Попри те, що спочатку такі системи були орієнтовані винятково на вивчення основ стрільби, сьогоденні VSAT-платформи здатні моделювати повноцінні тактичні взаємодії: ведення вогню з укриття, ухилення, прийняття рішень у стресових умовах, розпізнавання ситуацій «стріляти/не стріляти» (shoot/no-shoot), координацію дій кількох стрільців одночасно, зміну позицій під вогнем та аналіз точності вогню на рівні всієї команди (табл. 1).

Таблиця 1

Порівняння сучасних систем цифрової стрілецької імітації бою

Назва системи	Виробник	Основні можливості	Сфери застосування	Переваги
MantisX	Mantis	Графічний та числовий аналіз пострілу, рекомендації щодо покращення техніки, аналіз стабільності, точності, часу реакції	Індивідуальна стрілецька підготовка, оцінювання бойової ефективності	Реальний час, без використання боєприпасів, портативність
VSAT (Virtual Small Arms Trainer)	Різні (Thales, Guardiaris тощо)	Імітація бойових сценаріїв, аналіз дій стрільця в реальному часі, модульність	Тактична підготовка, групові тренування	Реалістичне середовище, підтримка різних типів зброї
Ground Combat Indoor Trainer (GCIT)	Saab	Тренування індивідуальної та групової стрільби, аналіз поведінки зброї	Групові тактичні тренування	Аналіз помилок у реальному часі, підтримка динамічних цілей
Small Arms Tactical Trainer (SATT)	Guardiaris	Оцінка стрільби в урбанізованому середовищі, інфрачервоний трекінг	Урбанізовані бойові сценарії	Висока точність трекінгу, панорамне зображення
Indoor Simulated Marksmanship Trainer (ISMT III)	InVeris Training Solutions	Моделювання вогневих дій, підтримка мінометів, бойові сценарії	Комплексне бойове моделювання	Незалежність від погодних умов, висока реалістичність
Smokeless Range Trainer (SRT)	Невідомий	Тестування точності та стабільності без боєприпасів	Індивідуальна підготовка	Економія ресурсів, контрольоване середовище
SRCE/SURVIVR	InVeris Training Solutions	360-градусне AR/VR середовище моделювання складних бойових умов	Тактична підготовка, групові операції	Повне занурення, підтримка складних сценаріїв

На заключення, слід зазначити, що впровадження цифрових технологій у процеси оцінювання бойової ефективності короткоствольної стрілецької зброї є не просто технологічною модернізацією традиційних підходів, а стратегічно важливою складовою адаптації збройних сил до викликів, що виникають у ході еволюції бойових дій сьогодення, де темп, точність і швидкість адаптації до змін умов обстановки, високий рівень підготовки військовослужбовця стали ключовими чинниками успіху на полі бою.

Висновки. Досліджено потенціал оптико-електронних систем, віртуальних тренажерів та інтерактивних платформ типу MantisX, SATT, VSAT, ISMT III, SRCE тощо. Ці технології дають змогу не лише моделювати різноманітні бойові сценарії, а й точно фіксувати ключові показники стрільби: момент натискання на спусковий гачок, рух ствола, етапи прицілювання, координати передбачуваного влучання, швидкість реакції та кінематику пострілу. Вивчено ефективність використання таких систем для побудови адаптивних тренувальних комплексів, що враховують змінні умови: освітлення, просторові обмеження, фоновий шум, стан стрільця (як фізичний, так і психологічний), а також взаємодію з союзниками й протидію противника.

Показано, що цифрова реєстрація бойових дій через вбудовані сенсори та системи трекінгу має великий аналітичний потенціал. Вона дозволяє виявити прямі зв'язки між поведінкою стрільця, конструктивними особливостями зброї та загальною результативністю

стрільби. На основі цього розроблено науково обґрунтовану методологію застосування технологій сухого вогню, лазерних тренажерів, інфрачервоної візуалізації та біометричного супроводу в рамках єдиного цифрового простору, здатного збирати, обробляти та аналізувати великі масиви бойових даних.

Встановлено, що широке застосування сучасних VSAT-систем значно перевершує можливості традиційних методів навчання стрільців. Такі системи дозволяють моделювати складні бойові умови, використовуючи елементи доповненої та віртуальної реальності, а також реалізовувати багаторівневу оцінку, від техніки окремого стрільця до взаємодії групи в умовах віртуального полігону. Результатом стало формування нового підходу до аналізу бойової ефективності короткоствольної зброї, який розглядає її як динамічний процес, що залежить від контексту. Основою цього підходу є інтеграція сенсорних, аналітичних, інформаційних та візуалізаційних компонентів у єдину цифрову екосистему бойової підготовки.

ЛІТЕРАТУРА:

1. Казначеев Д. Г., Волков Ю. М. Особенности идеомоторного тренирования под час вогневої підготовки. Юридичний науковий електронний журнал. 2022. № 11. С. 491-494. DOI: <https://doi.org/10.32782/2524-0374/2022-11/102>
2. Наточій А. Д., Болгаренко В. М. Вогнева підготовка та формування професійних якостей у майбутніх офіцерів: взаємозв'язок та взаємозалежність. Аналітично-порівняльне правознавство. 2024. № 3. С. 64-72. DOI: <https://doi.org/10.24144/2788-6018.2024.03.64>
3. Сучасні види вогнепальної стрілецької зброї підрозділів МВС України : навчальний посібник / Ю. Р. Йосипів, В. М. Синенький, М. Д. Курляк, М. О. Лиса, Н. Д. Туз, П. С. Вербицький, за заг. ред. Ю. Р. Йосипіва. Львів: Львівський державний університет внутрішніх справ, 2022. 184 с.
4. Хацаюк О., Самсонов Ю., Самсонова Г. Підготовка інструкторів з вогневої підготовки : колект. моногр. London-Chisinau : Dodo Books Indian Ocean Ltd. and OmniScriptum S.R.L. publishing group, 2024. 81 с.
5. Anderson M. Small arms training simulators in the New Zealand Defence Force. Defence Technology Agency, New Zealand Defence Force. Paper presented at DHSS 2014 (International Defense and Homeland Security Simulation Workshop). 2014. p. 7-12.
6. Chandan R.H., Sharmin N., Munir M.B., Razzak A., Naim T.A., Mubashshira T., Rahman M. AI-based small arms firing skill evaluation system in the military domain. Defence Technology. 2023. vol. 29, issue 9. p. 164–180. <https://doi.org/10.1016/j.dt.2023.02.024>
7. Fedaravičius A., Pilkauskas K., Slizys E., Survila A. Research and development of training pistols for laser shooting simulation system. Defence Technology. 2020. vol. 16, issue 3. p. 530-534
8. Laser Shot. Virtual Specialized Training Simulations (Law Enforcement Virtual Specialized Training Simulations). Laser Shot (SecurityTrainingE3). 2024. <https://securitytraining3.com/wp-content/uploads/2024/11/Law-Enforcement-Virtual-Specialized-Training-Simulations.pdf>
9. Lee B., Hwang T.Y., Hyun S., Lee H. Improvement of K-2 rifle's live-fire accuracy using virtual reality shooting training system. Virtual Reality. 2025. vol. 29. article 23. <https://doi.org/10.1007/s10055-024-01094-w>
10. Makedon V., Myachin V., Plakhotnik O., Fisunen N., Mykhailenko O. Construction of a model for evaluating the efficiency of technology transfer process based on a fuzzy logic approach. Eastern-European Journal of Enterprise Technologies. 2024. no 2(13(128)). pp. 47-57. <https://doi.org/10.15587/1729-4061.2024.300796>
11. Marino C. Reality Check: Haptics improvements to Army simulation training makes virtual environments feel more realistic. Army AL&T Magazine. Spring. 2025. p. 18–21. URL: <https://www.lineofdeparture.army.mil/Journals/Army-AL-T/AL-T-Archive/Spring-2025/Reality-Check/>
12. Marlok T., Takács M.G. VR Training Opportunities in the Hungarian Defence Forces. Academic and Applied Research in Military and Public Management Science (AARMS). 2024. vol. 23, no 2, pp. 19–37. <https://doi.org/10.32565/aarms.2024.2.2>
13. Nash T. Virtually Shooting Straight: modern Virtual Small Arms Trainer evolves from marksmanship to integrated squad-level tactical training. European Security & Defence. 2024. no 5. URL: <https://euro-sd.com/2024/05/articles/technology/38268/virtually-shooting-straight/>

14. Nautilus International Risk Consultants Ltd. Weapon simulation training services: VirTra recoil-kits, roundless laser weapon conversion, judgemental training simulators, battlefield effects. Nautilus International. 2024. <https://nautilus-intl.co.uk/portfolio/weapon-simulation/>

15. Rondón Gómez L.A., Alarcón P., Arce D. Design and Implementation of a Low-Cost Virtual Rifle Shooting Simulator for the Peruvian Army Military School. In 5th International Conference on Electrical, Communication and Computer Engineering (ICECCE 2024). Kuala Lumpur, Malaysia: Institute of Electrical and Electronics Engineers Inc. 2024. <https://doi.org/10.1109/ICECCE63537.2024.10823594>

REFERENCES:

1. Kaznacheiev D. H., Volkov Y. M. (2022), “Osoblyvosti ideomotornoho navchannia pid chas vohnevoi pidhotovky” [Peculiarities of ideomotor training during firearms training], *Yurydychnyi naukovyi elektronnyi zhurnal – Legal Scientific Electronic Journal*, no. 11, pp. 491–494. DOI: <https://doi.org/10.32782/2524-0374/2022-11/102>.

2. Natochii A. D., Bolharenko V. M. (2024), “Vohneva pidhotovka ta formuvannia profesiinykh yakosti u maibutnikh ofitseriv: vzaïmozv'язok ta vzaïmozalezhnist” [Fire training and development of professional qualities in future officers: interrelation and interdependence], *Analitichno-porivnialne pravoznavstvo – Analytical and Comparative Jurisprudence*, no. 3, pp. 64–72. DOI: <https://doi.org/10.24144/2788-6018.2024.03.64>.

3. Yosypiv Yu. R., Synenkyi V. M., Kurliak M. D., Lysa M. O., Tuz N. D., Verbytskyi P. S. (2022), *Suchasni vydy vohnepalnoi strilets'koi zbroi pidrozdiliv MVS Ukrainy* [Modern types of firearms of the units of the Ministry of Internal Affairs of Ukraine], Yu. R. Yosypiv (Ed.), Lviv: Lvivskyi derzhavnyi universytet vnutrishnikh sprav, 184 p.

4. Khatsaiuk O., Samsonov Yu., Samsonova H. (2024), *Pidhotovka instruktoriv z vohnevoi pidhotovky* [Training of firearms instructors], collective monograph, London–Chisinau: Dodo Books Indian Ocean Ltd. and OmniScriptum S.R.L. publishing group, 81 p.

5. Anderson M. (2014), “Small arms training simulators in the New Zealand Defence Force”, Paper presented at DHSS 2014 (International Defense and Homeland Security Simulation Workshop), Defence Technology Agency, New Zealand Defence Force, pp. 7–12.

6. Chandan R. H., Sharmin N., Munir M. B., Razzak A., Naim T. A., Mubashshira T., Rahman M. (2023), “AI based small arms firing skill evaluation system in the military domain”, *Defence Technology*, vol. 29, issue 9, pp. 164–180. <https://doi.org/10.1016/j.dt.2023.02.024>.

7. Fedaravičius A., Pilkauskas K., Slizys E., Survila A. (2020), “Research and development of training pistols for laser shooting simulation system”, *Defence Technology*, vol. 16, issue 3, pp. 530–534. <https://doi.org/10.1016/j.dt.2019.06.018>.

8. Laser Shot (2024), “Virtual Specialized Training Simulations (Law Enforcement Virtual Specialized Training Simulations)”, Laser Shot (SecurityTrainingE3). <https://securitytraining3.com/wp-content/uploads/2024/11/Law-Enforcement-Virtual-Specialized-Training-Simulations.pdf>.

9. Lee B., Hwang T. Y., Hyun S., Lee H. (2025), “Improvement of K-2 rifle’s live fire accuracy using virtual reality shooting training system”, *Virtual Reality*, vol. 29, article 23. <https://doi.org/10.1007/s10055-024-01094-w>.

10. Makedon V., Myachin V., Plakhotnik O., Fisunen N., Mykhailenko O. (2024), “Construction of a model for evaluating the efficiency of technology transfer process based on a fuzzy logic approach”, *Eastern-European Journal of Enterprise Technologies*, no. 2(13(128)), pp. 47–57. <https://doi.org/10.15587/1729-4061.2024.300796>.

11. Marino C. (2025), “Reality Check: Haptics improvements to Army simulation training makes virtual environments feel more realistic”, *Army AL&T Magazine*, Spring, pp. 18–21. <https://www.lineofdeparture.army.mil/Journals/Army-AL-T/AL-T-Archive/Spring-2025/Reality-Check/>.

12. Marlok T., Takács M. G. (2024), “VR Training Opportunities in the Hungarian Defence Forces”, *Academic and Applied Research in Military and Public Management Science (AARMS)*, vol. 23, no. 2, pp. 19–37. <https://doi.org/10.32565/aarms.2024.2.2>.

13. Nash T. (2024), “Virtually Shooting Straight: modern Virtual Small Arms Trainer evolves from marksmanship to integrated squad level tactical training”, *European Security & Defence*, no. 5. <https://euro-sd.com/2024/05/articles/technology/38268/virtually-shooting-straight/>.

14. Nautilus International Risk Consultants Ltd. (2024), “Weapon simulation training services: VirTra recoil kits, roundless laser weapon conversion, judgemental training simulators, battlefield effects”, Nautilus International. <https://nautilus-intl.co.uk/portfolio/weapon-simulation/>.

15. Rondón Gómez L. A., Alarcón P., Arce D. (2024), "Design and Implementation of a Low Cost Virtual Rifle Shooting Simulator for the Peruvian Army Military School", In: 5th International Conference on Electrical, Communication and Computer Engineering (ICECCE 2024), Kuala Lumpur, Malaysia: Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/ICECCE63537.2024.10823594>.

Ph.D. Lutsyshyn A.M., Ph.D. Loza V.M., Vasylenko Y.Y., Kondratiuk V.V.

DIGITAL TECHNOLOGIES IN DEVELOPING A METHODOLOGY FOR ASSESSING THE COMBAT EFFECTIVENESS OF SHORT-BARRELED SMALL ARMS

The article is devoted to the study of digital technologies for evaluating the combat effectiveness of short-barreled small arms in real and simulated combat environments. It analyzes the evolution of virtual small arms training simulators and their role in enhancing the accuracy of shooting analysis and tactical training. The purpose of the study is to determine the effectiveness level of using digital systems to ensure objective assessment of weapon technical parameters and to improve tactical approaches to their combat use. A systematic review of modern virtual training systems was conducted, including optoelectronic sensors, laser simulators, infrared tracking technologies, and AR/VR systems. The methodology is based on comparative analysis of system functionalities, their capability to capture shooting parameters (barrel trajectory, stability, reaction time), and process data using specialized software. The research results demonstrate that digital technologies provide high-precision recording of key shooting parameters such as barrel deviation, trigger pull timing, and shot dispersion, which enables identification of design flaws in weapons. These systems also make it possible to model dynamic combat scenarios, including urban environments and stress-inducing conditions, offering a comprehensive analysis of both individual and group tactical actions. The scientific novelty lies in the integration of sensor platforms, game engines, and biometric data (heart rate, stress level) to create a digital profile of combat effectiveness that takes into account both technical and physiological factors. The proposed approach opens new possibilities for objective comparison of different weapon models and their adaptation to contemporary combat doctrines. Future research perspectives include the development of simulation-supported systems to increase immersion in virtual environments. Further progress is expected in the formation of a unified digital assessment model that integrates data on individual and group tactical interactions to generate comprehensive combat profiles.

Keywords: short-barreled weapons, combat effectiveness, digital technologies, firearms training, virtual simulators, sensor systems, application tactics, tactical modeling.

РОЗВИТОК АРТИЛЕРІЙСЬКОЇ ТАКТИКИ У ЛОКАЛЬНИХ ТА МАСШТАБНИХ КОНФЛІКТАХ

Стаття присвячена дослідженню розвитку артилерійської тактики у контексті локальних та масштабних збройних конфліктів, із урахуванням досвіду провідних армій світу та особливостей сучасного ведення війни. Проаналізовано історичні та сучасні підходи до організації і застосування артилерії, включно з методами масованого вогневого ураження, високоточної стрільби, маневру вогнем та силами, а також взаємодії з іншими родами військ. Висвітлено вплив розвитку розвідувально-ударних комплексів, автоматизованих систем управління вогнем і новітніх засобів розвідки на ефективність артилерійських операцій у різних типах бойових дій.

У статті наведено порівняльний аналіз тактичних прийомів артилерії у локальних конфліктах низької інтенсивності та масштабних воєнних кампаніях. Розкрито роль артилерії у забезпеченні вогневої переваги та підтримки наступальних і оборонних операцій, а також у веденні контрбатареїної боротьби. Окремо приділено увагу впливу географічних та кліматичних умов на застосування артилерії та особливостям логістичного забезпечення в різних умовах.

Проаналізовано наукові та практичні підходи до удосконалення артилерійської тактики, зокрема на основі досвіду воєн останніх десятиліть (Ірак, Афганістан, Сирія, війна в Україні) та рекомендацій військових дослідних центрів НАТО і провідних вітчизняних наукових установ. Розглянуто шляхи інтеграції артилерійських підрозділів у систему мережоцентричних операцій та застосування безпілотних літальних апаратів для коригування вогню.

За результатами дослідження сформульовано пропозиції щодо підвищення ефективності артилерійських дій у сучасних умовах, удосконалення системи підготовки особового складу, впровадження новітніх технологій у розвідку, управління та коригування вогню. Запропоновано рекомендації для адаптації тактичних рішень артилерії до умов гібридних та асиметричних воєнних конфліктів, а також створення гнучкої доктрини застосування артилерії, здатної ефективно функціонувати як у локальних, так і у масштабних бойових діях.

Ключові слова: артилерія, артилерійська тактика, локальні конфлікти, масштабні конфлікти, вогнева підтримка, контрбатареїна боротьба, автоматизовані системи управління вогнем, розвідка, високоточна зброя.

Вступ та постановка завдання. Артилерія залишається основним засобом вогневого ураження противника у сучасних збройних конфліктах. За статистичними даними, у війні в Україні 2014–2025 років до 80 відсотків втрат живої сили і техніки противника завдається саме артилерією. Аналогічні дані спостерігаються в інших конфліктах кінця XX – початку XXI століття, зокрема в Іраку, Афганістані та Сирії, де артилерія відігравала провідну роль у забезпеченні вогневої переваги. Висока вогнева міць, здатність вести тривалі бої, підтримувати наступальні та оборонні операції, а також здійснювати контрбатареїну боротьбу роблять артилерію ключовим елементом сучасних бойових дій [1, 2].

Характер сучасних конфліктів має суттєві відмінності, що впливає на тактику застосування артилерії. У локальних війнах, які зазвичай характеризуються низькою або середньою інтенсивністю бойових дій та обмеженими фронтами, першочергове значення мають висока мобільність артилерійських підрозділів, прихованість вогневих позицій, швидка зміна місць ведення вогню, а також застосування високоточної зброї у поєднанні з безпілотними літальними апаратами для розвідки та коригування. У масштабних війнах пріоритетними залишаються масовані артилерійські удари, здатність тривалий час

утримувати інтенсивний темп вогню, тісна взаємодія з танковими, мотопіхотними та авіаційними підрозділами.

Розвиток військових технологій останніх десятиліть кардинально змінює вимоги до артилерії. В умовах мережочентричної війни ключовим чинником успіху стає швидкість передачі інформації, автоматизація процесів управління вогнем та інтеграція артилерії у єдину систему розвідки та ураження цілей. Застосування безпілотних літальних апаратів тактичного і оперативного рівня дає змогу значно скоротити час від виявлення цілі до відкриття вогню, який нині вимірюється не хвилинами, а секундами. Паралельно з цим зростає значення ефективної контрбатареїної боротьби, у якій перевага належить підрозділам, здатним максимально швидко виявляти, визначати координати та уражати артилерійські системи противника.

Попри суттєвий технологічний прогрес, проблема уніфікації тактичних підходів до застосування артилерії залишається актуальною. Відсутність єдиної, адаптивної доктрини, яка б враховувала досвід як локальних, так і масштабних конфліктів, призводить до ризиків неефективного використання артилерійських ресурсів, перевитрати боєприпасів, підвищення вразливості підрозділів та втрати ініціативи на полі бою. У сучасних умовах важливо забезпечити баланс між масованим вогнем і точковим ураженням, між мобільністю і стійкістю бойових порядків, між класичними прийомами і новітніми технологічними можливостями [3-5].

Метою цього дослідження є комплексний аналіз розвитку артилерійської тактики в умовах локальних та масштабних конфліктів і вироблення практичних рекомендацій щодо її удосконалення для підвищення бойової ефективності артилерії у Збройних Силах України. У межах роботи планується оцінити сучасний стан і тенденції розвитку артилерійської тактики на основі досвіду збройних конфліктів останніх десятиліть, визначити відмінності тактичних підходів у локальних війнах та масштабних бойових діях, проаналізувати вплив новітніх технологій – безпілотних літальних апаратів, високоточних боєприпасів, автоматизованих систем управління вогнем і сучасних засобів контрбатареїної боротьби – на ефективність артилерії [5-14]. На основі проведеного аналізу будуть сформульовані пропозиції щодо удосконалення бойових статутів і методичних рекомендацій із застосування артилерії, а також запропоновано комплекс заходів, спрямованих на підвищення мобільності, точності та живучості артилерійських підрозділів у різних типах конфліктів.

Аналіз останніх нормативних документів, досліджень та публікацій. Нормативно-правова база, яка регламентує питання організації та застосування артилерії у Збройних Силах України, а також підготовки та функціонування артилерійських підрозділів у бойових умовах, ґрунтується на таких основних документах:

1. Бойовий статут Сухопутних військ Збройних Сил України (частини II та III). Визначає основи організації і ведення загальновійськового бою, зокрема порядок застосування артилерії в обороні та наступі, організацію вогневої підтримки, взаємодію з іншими родами військ і службами, а також заходи маскування, маневру вогнем і силами.

2. Статут артилерії Збройних Сил України. Регламентує завдання, організацію та порядок бойового застосування артилерії у різних видах бою, правила ведення вогню, контрбатареїної боротьби, а також визначає порядок планування вогневих завдань.

3. Керівництво з бойової роботи артилерії. Містить докладні інструкції щодо організації вогню, розвідки цілей, підготовки вогневих позицій, проведення вогневих нальотів, коригування стрільби, а також взаємодії з розвідувальними та авіаційними підрозділами.

4. НАТО ATP-3.2.1 «Artillery Procedures» та STANAG 2934 «Counter-Battery Operations». Визначають стандартизовані процедури планування та застосування артилерії у багатонаціональних операціях, включно з організацією контрбатареїної боротьби, інтеграцією артилерії у систему вогневої підтримки, а також використанням автоматизованих систем управління вогнем.

5. AJP-3.2 «Allied Joint Doctrine for Land Operations». Містить концептуальні основи інтеграції артилерії у багатодоменні операції та визначає місце артилерії у сучасних мережоцентричних бойових діях.

Аналіз зазначених документів показує, що вітчизняна нормативно-правова база загалом врегульовує основні питання організації та ведення артилерійського вогню в умовах локальних та масштабних конфліктів. Водночас у національних документах бракує єдиного підходу до інтеграції новітніх технологій, зокрема безпілотних літальних апаратів, автоматизованих систем управління вогнем і високоточної зброї, у єдину доктрину артилерійських дій. Недостатньо врегульованими залишаються питання адаптації тактики артилерії до умов гібридних конфліктів та сучасної контрбатарейної боротьби.

Численні наукові праці українських військових дослідників, зокрема О. Драпатого, С. Соколовського, В. Паценка, присвячені питанням підвищення ефективності вогневої підтримки, удосконалення системи контрбатарейної боротьби та впровадження досвіду сучасних конфліктів у навчальний процес. Значна увага приділяється аналізу зарубіжного досвіду, особливо армій США, Великої Британії, Польщі та країн Балтії, які активно розвивають концепцію мережоцентричного застосування артилерії та інтеграцію засобів розвідки у бойові процеси.

У роботах військових наукових центрів, зокрема Національного університету оборони України, уточнюється місце артилерії у структурі вогневого ураження противника, формулюються функції артилерії у різних видах бою та визначається її роль у забезпеченні оперативної та тактичної переваги. Дослідження, присвячені критеріям оцінки ефективності артилерійських дій, пропонують систематизований підхід до визначення рівня вогневої ефективності, живучості підрозділів та швидкості виконання вогневих завдань.

Застосування цих напрацювань у поєднанні з міжнародними стандартами дозволить більш точно визначати фактичний стан бойової готовності артилерійських підрозділів, своєчасно виявляти та реалізовувати резерви для підвищення ефективності артилерійських дій у локальних та масштабних конфліктах.

Мета статті полягає у вирішенні таких науково-практичних завдань:

- здійснити порівняльний аналіз артилерійської тактики у локальних конфліктах низької інтенсивності та масштабних бойових діях;
- охарактеризувати основні підходи до організації застосування артилерії, включно з методами масованого вогню, високоточної стрільби, маневру вогнем та силами, а також взаємодії з іншими родами військ;
- проаналізувати вплив новітніх технологій – автоматизованих систем управління вогнем, безпілотних літальних апаратів, високоточної зброї та систем розвідки – на ефективність артилерійських дій;
- оцінити сучасний стан нормативно-правової та доктринальної бази застосування артилерії у Збройних Силах України з урахуванням стандартів НАТО та досвіду провідних армій світу;
- сформулювати практичні рекомендації щодо підвищення ефективності артилерійських підрозділів у ЗСУ шляхом удосконалення тактики, логістики, підготовки особового складу та інтеграції артилерії у мережоцентричні операції.

Реалізація цих завдань має сприяти розширенню наукового розуміння сучасної артилерійської тактики та розробці шляхів її адаптації до умов гібридних і повномасштабних збройних конфліктів, що дозволить підвищити ефективність застосування артилерії у системі вогневого ураження противника.

Виклад основного матеріалу. Зі здобуттям незалежності Україна має можливість самостійно вирішувати свою долю, формувати зовнішню і внутрішню політику, розвивати усі сфери життя, зокрема Збройні Сили як основу обороноздатності держави. Задля цього триває реформування Збройних Сил України з урахуванням національних інтересів держави.

Індустріальна революція сприяла появі лиття з цілісної сталі, вдосконаленню нарізних стволів, вдосконаленню пороху – усе, що забезпечило більшу точність, дальність та

надійність артилерійських систем.

Артилерія здавна вважається «богом війни». Проте саме з початком Першої світової війни (1914–1918) її роль в бойових діях набула нового масштабу, перетворивши артилерію на основну силу на полі бою. У подальші десятиліття її розвиток відзначався переходом від масованих обстрілів до точкових високотехнологічних ударів, а також значною автоматизацією та цифровізацією систем управління вогнем.

До Першої світової війни артилерія здебільшого застосовувалась як допоміжний засіб підтримки піхоти. Однак статична позиційна війна на Західному фронті змінила характер бойових дій: фронтова лінія стабілізувалась, а прорвати укріплені позиції без масованого артилерійського вогню стало неможливо. Тому обидві сторони почали активно нарощувати артилерійський потенціал.

У Першій світовій війні були застосовані десятки тисяч гармат, гаубиць та мінометів. Наприклад, під час битви на Соммі 1916 року британські війська провели попередню артилерійську підготовку тривалістю сім діб, випустивши понад 1,5 мільйона снарядів. Це стало символом нової фази – війни артилерії, де головна увага приділялася масованому, але не завжди точному вогню.

Однак артилерія того часу мала обмежену мобільність та низьку точність. Координація вогню була ускладнена відсутністю сучасних засобів зв'язку та розвідки. Попри це, саме вона була головним чинником втрат: за різними оцінками, до 70% усіх поранень і смертей були спричинені артилерійським вогнем [7].

Ключові інновації:

- застосування відкатних механізмів, що дозволили зберегти приціл після пострілу та підвищити темп;
- введення індивідуального надання обчислень і роботи спостерігачів у польоту, що дозволило перейти до непрямої стрільби;
- широке використання 155 мм De Bange (рис. 1) у французькій армії, хоча застарілих, як базової контрбатареїної системи в перші роки війни;
- застосування гігантських облогових гармат, таких як австро-угорські Škoda 305 мм (рис. 2).

Отже, Перша світова війна стала вершиною масових, проте неточних артилерійських обстрілів, що стимулювало пошук нових тактичних і технічних рішень.



Рисунок 1 – 155 мм De Bange



Рисунок 2 – Škoda 305 мм

На початку війни координація між артилерією та піхотою була слабкою. Лише до 1917–1918 років союзники почали застосовувати рухомі вогневі вали – послідовні обстріли, які просувалися разом із атакуючими піхотними підрозділами. Це зменшувало втрати й дозволяло проривати оборону без тривалого перебування під кулеметним вогнем. Масове застосування снарядів і нових типів боєприпасів.

Перша світова стала війною артилерійської індустрії. Усі сторони почали масово виробляти не тільки уламкові та фугасні снаряди, а й отруйні гази, які запускалися з

артилерійських систем. Газові атаки, розпочаті німцями в 1915 році під Іпром, стали ще однією функцією артилерії – засобом хімічного ураження.

У 1920–1930-х роках відбувається переосмислення ролі артилерії. З'являються механізовані тягачі, що підвищують мобільність гармат, а також самохідні артилерійські установки. У Другій світовій війні (1939–1945) артилерія знову відіграла ключову роль. Проте вона стала більш інтегрованою в загальновійськові операції, зокрема у підтримці танкових проривів і наступів.

Німеччина активно застосовувала штурмові гармати (Sturmgeschütz), США – самохідні гаубиці типу M7 Priest (рис. 3), СРСР – відомі САУ СУ-76 і СУ-152 (рис. 4).



Рисунок 3 – M7 Priest



Рисунок 4 – СУ-152

Особливу увагу приділяли розвідці та коригуванню вогню – з'являються артилерійські спостерігачі, спеціалізовані літаки-коригувальники, що дозволяли підвищити точність вогню.

Важливою зміною став розвиток ракетної артилерії. Радянські «Катюші» (рис. 5) стали першим прикладом масового застосування реактивної системи залпового вогню, яка могла накрити вогнем велику площу за лічені секунди. Це дало змогу завдавати потужних ударів по живій силі та техніці противника при мінімальному часу перебування на позиції.



Рисунок 5 – БМ-13 «Катюша»

Після 1945 року почалася нова геополітична епоха – період Холодної війни, у якій провідні ролі відігравали США і СРСР. В умовах взаємного ядерного стримування артилерія стала не лише звичайним вогневим засобом, але й частиною ядерної тріади. У цей період з'являються артилерійські системи, здатні вести вогонь ядерними снарядами малого калібру [4].

Наприклад:

- **M110** (США) (рис. 6) – 203-мм самохідна гаубиця, здатна застосовувати ядерні снаряди W33.
- **2С7 «Піон»** (СРСР) (рис. 7) – 203-мм САУ, одна з найпотужніших на той час, з дальністю стрільби до 47 км.



Рисунок 6 – М110 (США)



Рисунок 7 – 2С7 «Піон» (СРСР)

Ці системи мали виконувати роль тактичного стримування у випадку конфлікту високої інтенсивності в Європі [3].

Після завершення Другої світової війни провідні військові держави світу – передусім США та СРСР – опинились у новому стратегічному середовищі, яке вимагало переосмислення принципів застосування артилерії. На зміну масованому вогню по площах прийшов запит на точкове ураження в умовах обмеженого часу на прийняття рішень. У цій трансформації ключову роль відіграла автоматизація процесів управління вогнем, розвиток засобів обчислення балістики, застосування лазерної техніки та електроніки. Починаючи з 1960-х років, зміни у технічному оснащенні артилерії дедалі активніше впливали на еволюцію тактики її застосування. Розробка автоматизованих балістичних обчислювачів, лазерних далекомірів та електронних систем управління вогнем у США, СРСР, а згодом і в інших країнах сприяла зростанню швидкості бойової реакції та точності [8]. Це радикально змінило уявлення про ефективність артилерії в бою: на заміну об'ємному вогню по квадратах приходив вогонь по точних координатах, з урахуванням реальних умов ведення вогню, метеорології, рельєфу, відстані та навіть руху цілі. Тактична гнучкість артилерійських підрозділів зросла, а сама артилерія перетворилася на один із головних інструментів маневреного бою.



Рисунок 8 – 122-мм гаубиця Д-30

В'єтнамська війна (1955–1975) стала першим конфліктом, де тактичне застосування артилерії зіграло важливу роль у боротьбі проти нерегулярних сил. США активно використовували артилерійські бази підтримки (fire support bases), які розташовувалися у джунглях і забезпечували мобільну підтримку бойових дій піхоти. Вогонь вівся переважно з гаубиць калібру 105 мм і 155 мм. Швидке розгортання, концентрація вогню, використання авіаційної розвідки – ці елементи лягли в основу майбутніх моделей застосування артилерії в умовах локальних конфліктів [6].

У 1970–1980-х роках, на фоні афганської війни (1979–1989) (рис. 9), радянські війська адаптували артилерійську тактику до гірської місцевості та боротьби з партизанськими формуваннями. Самохідна артилерія, міномети, буксирувані гармати активно застосовувались не лише для безпосередньої підтримки військ, а й для блокування маршрутів постачання, обстрілу таборів та контролю важливих вузлів. Особливої ваги набув «вогневий вал» – одночасне масоване обстрілювання потенційного району розташування противника. Водночас використання розвідки, в тому числі агентурної, мало велике значення для успішного застосування артилерії, а елементи артилерійської розвідки впроваджувались навіть на батальйонному рівні [8].



Рисунок 9 – Війна в Афганістані 1979-1989

[7].



Рисунок 10 – Війна Судного дня 1973 року

У арабо-ізраїльських війнах (особливо у Війні Судного дня 1973 року) (рис. 10) артилерія стала головним чинником у стримуванні масованих танкових атак. Ізраїльська армія показала ефективність високоточної координації артилерії з авіацією і танками. Для цього були застосовані елементи глибокої автоматизації управління вогнем – швидка передача координат, централізоване управління залпами, використання вогню на випередження. Артилерія вже не просто вела вогонь по готовим координатам, вона діяла як інтегрований компонент маневрової оборони та контратак [7].

З розпадом СРСР і закінченням Холодної війни у 1990-х роках починається перехід до так званої "артилерії нового покоління". У конфліктах на Балканах, у Чечні, Іраку, Афганістані 2000-х років тактика використання артилерії адаптується до нових загроз: асиметричних бойових дій, урбанізованого середовища, партизанської тактики. Перевага віддається мобільності, точності, інформаційній перевазі.

В операції "Буря в пустелі" (1991) (рис. 11), США продемонстрували нову концепцію застосування артилерії – як частини скоординованого глибокого удару. Авіація, ракетні війська, РСЗВ, самохідна артилерія діяли за єдиним сценарієм – у рамках концепції "шоку та трепету" [4]. Тактика змістилась від традиційного артилерійського прориву до моделі, де артилерія забезпечувала динамічну підтримку маневруючих військ, із прицільними ударами по центрах управління, логістичних вузлах, зонах скупчення техніки. Поява перших керованих боєприпасів (наприклад, Copperhead) та супутникових засобів наведення суттєво змінила вимоги до підготовки артилерійських підрозділів і їхнього зв'язку з розвідкою.



Рисунок 11 – Буря в пустелі 1991

У чеченських війнах (1994–1996, 1999–2009) російська артилерія часто застосовувалась у масштабних обстрілах урбанізованих зон. Основна тактика – знищення потенційних вогневих точок противника на випередження, не враховуючи колатеральні втрати. Водночас бойові дії в горах Чечні сприяли розвитку моделі "вогневого патруля" – тобто підтримки піхоти невеликими артилерійськими підрозділами, що діяли швидко, автономно, у складних умовах рельєфу.

Особливий поворот у тактичному мисленні стався після війни у Грузії (2008). Російські війська активно використовували артилерійську розвідку, безпілотники, централізоване управління вогнем з залученням автоматизованих систем. Це дало поштовх для вдосконалення таких АСУ, як "Капустник", а пізніше – "Акація-М" та "Ковчег". Завдання артилерії тепер – не просто масований вогонь, а точкове ураження при максимальній економії боєприпасів і зменшенні часу реагування.

Війна в Україні з 2014 року стала лабораторією нового типу артилерійської війни. З одного боку – використання застарілих буксируваних гармат, з іншого – активне впровадження цифрових систем управління вогнем, БПЛА, геоінформаційних платформ. Вже тоді були спроби використання коригованих снарядів "Квітник" та адаптованих до GPS боєприпасів. Водночас найважливішим стало відновлення втраченого в пострадянський час зв'язку між розвідкою та артилерією.

Із 2022 року, після початку повномасштабного вторгнення, війна набула характеру високоінтенсивного артилерійського протистояння. Обидві сторони широко застосовували РСЗВ, ствольну артилерію, дрони-розвідники та БПЛА-камікадзе. Україна стала прикладом, як в умовах технологічної асиметрії можна досягти переваги за рахунок інтеграції цивільних технологій (Starlink, DJI) із військовими системами управління вогнем. Системи "Кропива", "GIS Arta", "Артзалп", "Delta" дозволяють отримувати цілі в реальному часі та передавати їх артилерійським батареям менш ніж за 60 секунд. Тактична схема змінилася: артилерія діє малими підрозділами, переміщується після кількох пострілів, веде вогонь із неочікуваних позицій. Західна артилерія, така як PzH 2000, Caesar, M777, M109A6 Paladin, HIMARS, змусила російську сторону адаптуватися до нової реальності: вогонь ведеться точково, часто – по одиничних цілях, в умовах контрбатареїної боротьби. Артилерійські тактики тепер

включають: активне застосування дронів-коригувальників, зміну позицій після кожного залпу (Shoot and Scoot), приховування техніки за допомогою аерозольних завіс та маскувannya, використання артилерійської "засідки", цілевказання зі смартфонів. Одним із нововведень стала "цифрова батарея", коли кожна гармата має планшет або інший пристрій з геопросторовим інтерфейсом, що дозволяє одночасно, без командного пункту, координувати удар. Новітні технології, такі як штучний інтелект, вже використовуються для визначення пріоритетності в цілях і моделювання наслідків ударів – це стало реальністю саме у війні 2022–2025 років.



Рисунок 12 – Російсько-українська війна

Висновки. Проведене дослідження розвитку артилерійської тактики показало, що за останнє століття артилерія зазнала кардинальної трансформації, пройшовши шлях від громіздких гармат з неточними обстрілами по площах до високоточної, мобільної та інтегрованої у розвідувально-ударні комплекси системи вогневого ураження. У процесі цієї еволюції вирішальну роль відіграли три чинники: зміна характеру збройних конфліктів, технологічний прогрес та адаптація організаційно-тактичних структур до нових умов ведення бойових дій. Порівняльний аналіз локальних і масштабних конфліктів засвідчив суттєву різницю у підходах до застосування артилерії. У локальних війнах другої половини XX та початку XXI століть (В'єтнам, Афганістан, Ірак, Сирія) пріоритет надавався високій мобільності підрозділів та швидкій реакції на зміну обстановки. Артилерія діяла відносно малими групами, концентруючи вогонь по конкретних важливих цілях, часто у поєднанні з повітряною підтримкою та розвідувальною інформацією в режимі реального часу. У масштабних війнах (Друга світова війна, війна Судного дня 1973 р., операція «Буря в пустелі» 1991 р., війна в Україні 2014–2025 рр.) артилерія зберегла ключову роль у завданні масованих ударів, контрбатареїній боротьбі та підтримці великих наступальних і оборонних операцій.

Дослідження підтвердило, що сучасна тактика артилерії охоплює широкий спектр методів – від масованого вогню по площах до точкових ударів високоточними боєприпасами, від тривалих артилерійських підготовок до швидких маневрових операцій за принципом «Shoot and Scoot». Контрбатареїна боротьба набуває дедалі більшого значення, адже сучасні радіолокаційні станції, безпілотна розвідка та автоматизовані системи управління вогнем дозволяють виявляти позиції противника майже миттєво після відкриття вогню. Відповідно, живучість артилерійських підрозділів залежить від швидкості зміни позицій, ефективного маскувannya та застосування засобів радіоелектронної боротьби. Впровадження новітніх технологій докорінно змінило підходи до організації артилерійських операцій. Автоматизовані системи управління вогнем, безпілотні літальні апарати для розвідки й коригування, високоточні боєприпаси, засоби супутникової навігації та штучного інтелекту дозволили скоротити цикл «виявлення–ураження» до лічених хвилин, а в деяких випадках – до секунд. Зросла ефективність використання боєприпасів, зменшились втрати особового складу завдяки дистанційному управлінню та безекіпажним рішенням.

Український досвід 2014–2025 рр. довів, що інтеграція цифрових платформ («Кропива», GIS Arta, Delta) у процес управління артилерією значно підвищує ефективність взаємодії між розвідкою, вогневими засобами та командуванням [7]. Оцінка нормативно-правової та доктринальної бази показала, що в Україні існує розгалужена система документів, яка регламентує організацію й застосування артилерії (бойові статuti, керівництва, інструкції). Водночас сучасні виклики вимагають подальшої інтеграції в національну систему стандартів НАТО та розробки єдиної адаптивної доктрини застосування артилерії в умовах як класичних, так і гібридних воєн. Зокрема, важливим є включення положень про комплексне використання безпілотної розвідки, автоматизованих систем управління, високоточних боєприпасів та засобів РЕБ у єдиному оперативному контурі.

За результатами дослідження сформульовано низку практичних рекомендацій:

- розвивати національні автоматизовані системи управління артилерійським вогнем та забезпечувати їх повну інтеграцію з усіма розвідувальними засобами;
- збільшити частку високоточних боєприпасів у боєкомплекті артилерії, що дасть змогу ефективно знищувати високопріоритетні цілі з мінімальними витратами ресурсів;
- впроваджувати роботизовані артилерійські платформи та безекіпажні транспортні системи для постачання боєприпасів у зону бойових дій;
- удосконалювати систему контрбатарейної боротьби шляхом розгортання сучасних радіолокаційних станцій, дронів-розвідників та комплексів РЕБ;
- адаптувати програми підготовки особового складу з урахуванням досвіду мережоцентричних і гібридних конфліктів;
- створювати інтегровані навчальні центри для відпрацювання взаємодії артилерії з іншими родами військ у складі єдиної інформаційно-вогневої системи.

Майбутнє артилерії безпосередньо пов'язане з подальшою автоматизацією, використанням штучного інтелекту, автономних дронів-розвідників та роботизованих вогневих платформ. Головним завданням стане побудова єдиної інформаційно-вогневої системи, здатної діяти в режимі реального часу та забезпечувати миттєву передачу даних від сенсорів і розвідки до вогневих засобів. Така система дозволить значно скоротити час реагування, підвищити точність ударів і забезпечити вирішальну вогневу перевагу в будь-якому типі сучасного чи майбутнього конфлікту. Успішна реалізація цих підходів зробить артилерію ще більш смертоносною, мобільною та здатною діяти в умовах інтенсивного протистояння з противником, який також володіє високотехнологічними засобами ураження.

ЛІТЕРАТУРА:

1. Бойовий статут Сухопутних військ Збройних Сил України. Частина II. Артилерія. Затверджена наказом Командувача Сухопутних військ ЗСУ № 376 від 18.05.2020.
2. Методичні рекомендації «Артилерійський дивізіон в бою» (ВП 7-07(03)56.01) за досвідом операції Об'єднаних сил (раніше АТО). Київ : Центр оперативних стандартів і методики підготовки ЗС України; Командування Сухопутних військ ЗСУ; Головне управління доктрин та підготовки Генерального штабу ЗС України, грудень 2021. 209 с.
3. Трофименко П. Є., Пушкарьов Ю. І., Латін С. П., Ляпа М. М., Панченко О. В. *Тактична підготовка артилерійських підрозділів : підручник*. Суми: Сумський державний університет, 2012. 776 с. ISBN 978-966-657-446-9
4. Малишкін О. В., Босий О. Б., Григоренко С. А., Іванов Т. С., Галкін А. О. Рекомендації щодо підвищення бойової (вогневої) ефективності засобів ураження осколочної дії. Збірник наукових праць Військової академії (м. Одеса). 2021. Вип. 1(15). С. 107-114.
5. Міністерство оборони України. *Методичні рекомендації «Артилерійський дивізіон в бою» (ВП 7-07(03)56.01) за досвідом ООС*. Київ: Центр оперативних стандартів ЗСУ; Командування Сухопутних військ; Генштаб, грудень 2021. 209 с.
6. Трофімов І. В., Холін В. М. Проблеми бойового застосування РВіА в АТО та пропозиції щодо їх вирішення. // *Перспективи розвитку ракетних військ і артилерії Сухопутних військ : збірка тез доповідей* (5–6 листопада 2014 р.). Львів: Академія сухопутних військ, 2014. С. 14–18.

7. Кривов'яз А. Т., Зубков А. М. Напрями модернізації та підвищення точності бойового вогню РВіА. // *Тези конференції "Перспективи розвитку РВіА"* (Львів, 5–6.11.2014). Львів: Академія СВ, 2014. С. 30–35.
8. Петренко В. М., Ляпа М. М., Приходько А. І. та ін. *Засоби підготовки та управління вогнем артилерії* [Текст]: навч. посіб. – Суми: СумДУ, 2015. – 458 с.
9. Петренко В. М., Ляпа М. М., Житник В. Є. та ін. *Блокнот зі стрільби і управління вогнем артилерії* [Текст]: навч. посіб. – Суми: СумДУ, 2017. – 311 с. ISBN 978-966-657-659-3
10. Трофименко П. Є. та ін. *Тактична підготовка артилерійських підрозділів* [Текст]: підручник. – Суми: Сумський державний університет, 2012 (електронне вид.) – 776 с. ISBN 978-966-657-446-9
11. Міністерство оборони України (ред.). *Перспективи розвитку ракетних військ і артилерії Сухопутних військ*: зб. тез доп. наук.-техн. конф. 5–6 листопада 2014 р. – Львів: Академія Сухопутних військ, 2014. – 222 с.
12. *Боги війни*. Що означає емблема українських артилеристів // Nakypilo.ua. 2025. URL: nakypilo.ua – про символіку та історію емблеми артилеристів ЗСУ.
13. Історія артилерії: від ранніх форм до модерних систем // Babel.ua. 2022. ([дата перегляду: 2025]). – Популярно-наукова розповідь про розвиток артилерії, зокрема роль Густава II Адольфа у мобільності артилерії.
14. Ракетні війська та артилерія України // Вікіпедія (укр.). – Матеріал містить актуальні дані про структуру, роль і чисельність РВіА ЗСУ. Переглянуто 2025.

REFERENCES:

1. Combat Regulations of the Ground Forces of the Armed Forces of Ukraine. Part II. Artillery. Approved by order of the Commander of the Ground Forces of the Armed Forces of Ukraine No. 376 dated 05/18/2020.
2. Methodological recommendations "Artillery Division in Battle" (VP7 07(03)56.01) based on the experience of the Joint Forces Operation (formerly ATO). Kyiv: Center for Operational Standards and Training Methods of the Armed Forces of Ukraine; Command of the Ground Forces of the Armed Forces of Ukraine; Main Directorate of Doctrines and Training of the General Staff of the Armed Forces of Ukraine, December 2021. 209 p.
3. Trofymenko P.E., Pushkarev Y.I., Latin S.P., Lyapa M.M., Panchenko O.V. Tactical training of artillery units: textbook. Sumy: Sumy State University, 2012. 776 p. ISBN 978 966 657 446 9
4. Malyshkin, O. V., Bosyi, O. B., Hryhorenko, S. A., Ivanov, T. S. and Halkin, A. O., (2021). "Rekomendatsii shchodo pidvyshchennia boiovoi (vohnevoi) efektyvnosti zasobiv urazhennia oskolochnoi dii" [Recommendations for increasing the combat (fire) effectiveness of fragmentation weapons.]. Zbirnyk naukovykh prats Viiskovoi akademii (m. Odesa). No.1(15), pp.107–114.
5. Ministry of Defense of Ukraine. Methodological recommendations "Artillery Division in Battle" (VP7 07(03)56.01) based on the experience of the Joint Forces. Kyiv: Center for Operational Standards of the Armed Forces of Ukraine; Ground Forces Command; General Staff, December 2021. 209 p.
6. Trofimov I.V., Kholin V.M. Problems of combat use of R&A in the ATO and proposals for their solution. // Prospects for the development of missile forces and artillery of the Ground Forces: collection of abstracts of reports (November 5–6, 2014). Lviv: Academy of the Ground Forces, 2014. pp. 14–18.
7. Kryvov'яз A.T., Zubkov A.M. Directions for modernization and improvement of the accuracy of combat fire of R&A. // Abstracts of the conference "Prospects for the development of R&A" (Lviv, 5–6.11.2014). Lviv: Academy of the SV, 2014. pp. 30–35.
8. Petrenko V.M., Lyapa M.M., Prykhodko A.I. and others. Means of training and control of artillery fire [Text]: a textbook. – Sumy: SumDU, 2015. – 458 p.
9. Petrenko V.M., Lyapa M.M., Zhitnyk V.E. and others. Notebook on firing and control of artillery fire [Text]: a textbook. – Sumy: SumDU, 2017. – 311 p. ISBN978 966 657 659 3
10. Trofymenko P.E. et al. Tactical training of artillery units [Text]: textbook. – Sumy: Sumy State University, 2012 (electronic edition) – 776 p. ISBN978 966 657 446 9
11. Ministry of Defense of Ukraine (ed.). Prospects for the development of missile forces and artillery of the Ground Forces: collection of abstracts of the additional scientific and technical conference of November 5–6, 2014. – Lviv: Academy of the Ground Forces, 2014. – 222 p.
12. Gods of war. What does the emblem of Ukrainian artillerymen mean // Nakypilo.ua. 2025. URL: nakypilo.ua – about the symbolism and history of the emblem of the artillerymen of the Armed Forces of Ukraine.

13. History of artillery: from early forms to modern systems // Babel.ua. 2022. ([date of revision: 2025]). – A popular scientific story about the development of artillery, in particular the role of Gustav II Adolf in the mobility of artillery.

14. Missile Forces and Artillery of Ukraine // Wikipedia (ukr.). – The material contains current data on the structure, role and number of the Rocket and Artillery Forces of the Armed Forces of Ukraine. Revised 2025.

Ph.D. Koltsov R.U., Levinskova N.V., Kucher A.O.

DEVELOPMENT OF ARTILLERY TACTICS IN LOCAL AND LARGE-SCALE CONFLICTS

The article is devoted to the study of the development of artillery tactics in the context of local and large-scale armed conflicts, taking into account the experience of the world's leading armies and the features of modern warfare. Historical and modern approaches to the organization and use of artillery are analyzed, including methods of massive fire damage, high-precision shooting, maneuvering with fire and forces, as well as interaction with other branches of the armed forces. The impact of the development of reconnaissance and strike complexes, automated fire control systems and modern reconnaissance means on the effectiveness of artillery operations in various types of combat operations is highlighted.

The article provides a comparative analysis of artillery tactical techniques in local low-intensity conflicts and large-scale military campaigns. The role of artillery in providing fire superiority and supporting offensive and defensive operations, as well as in conducting counter-battery combat, is revealed. Special attention is paid to the influence of geographical and climatic conditions on the use of artillery and the peculiarities of logistical support in different conditions.

Scientific and practical approaches to improving artillery tactics are analyzed, in particular, based on the experience of wars of recent decades (Iraq, Afghanistan, Syria, the war in Ukraine) and recommendations of NATO military research centers and leading domestic scientific institutions. Ways of integrating artillery units into the system of network-centric operations and the use of unmanned aerial vehicles for fire correction are considered.

Based on the results of the study, proposals are formulated to increase the effectiveness of artillery operations in modern conditions, improve the personnel training system, and introduce the latest technologies in reconnaissance, fire control, and fire correction. Recommendations are proposed for adapting tactical artillery solutions to the conditions of hybrid and asymmetric military conflicts, as well as creating a flexible doctrine of artillery use that can function effectively in both local and large-scale combat operations.

Keywords: *artillery, artillery tactics, local conflicts, large-scale conflicts, fire support, counter-battery warfare, automated fire control systems, reconnaissance, high-precision weapons.*

МЕТОДИЧНІ ЗАСАДИ ПІДГОТОВКИ СТРІЛЬЦЯ ТА ВИКОРИСТАННЯ СТРІЛЕЦЬКОЇ ЗБРОЇ В УРБАНІЗОВАНИХ СЕРЕДОВИЩАХ

Стаття присвячена розробці методичних засад підготовки стрільців та ефективного використання стрілецької зброї в урбанізованих середовищах, де бойові дії характеризуються обмеженим простором, високою динамікою та складною просторовою конфігурацією. Дослідження ґрунтується на аналізі сучасного бойового досвіду, отриманого в урбанізованих театрах воєнних дій, та експериментальних випробуваннях на спеціалізованих полігонах і в середовищах віртуальної та доповненої реальності. Використовувалися методи структурного, імітаційного та ситуаційного моделювання для відтворення реальних умов міського бою, включаючи стрільбу в обмеженому просторі, з нестандартних положень та за наявності перешкод. У результаті дослідження встановлено, що ефективність стрілецької зброї в урбанізованих умовах визначається її точністю, пробивною здатністю, ергономічністю та адаптивністю до швидкоплинних бойових ситуацій, що підтверджено випробуваннями компактних штурмових гвинтівок і пістолетів-кулеметів. Наукова новизна полягає в обґрунтуванні методики оцінки, яка інтегрує аналіз балістичних характеристик, рикошетної безпеки, акустичної непомітності та психологічної готовності стрільця. Запропоновано нові підходи до моделювання бойових сценаріїв, що враховують багаторівневу структуру міських просторів і стрес-фактори. Отримані результати формують чіткі рекомендації щодо вибору оптимальних зразків зброї для підрозділів, що діють у міських умовах. Подальші дослідження спрямовані на вдосконалення віртуальних тренажерних комплексів із застосуванням біометричних сенсорів для оцінки психофізіологічного стану стрільця в реальних бойових умовах. Можливим напрямком є і розробка універсальних стандартів випробувань модульних систем озброєння для забезпечення їхньої ефективності в динамічних урбанізованих середовищах.

Ключові слова: стрілецька зброя, урбанізоване середовище, тактична підготовка, бойові дії в місті, ергономіка зброї, методика випробувань, ближній бій.

Вступ та постановка проблеми. Збройні конфлікти дедалі частіше розгортаються в урбанізованих середовищах, де щільна забудова, обмежений простір і багаторівнева структура створюють унікальні виклики для ведення бойових дій. Урбанізоване середовище, з його вузькими коридорами, багатоповерховими будівлями та численними перешкодами, вимагає від військовослужбовців високого рівня координації, швидкості реакції та вміння ефективно застосовувати зброю в умовах ближнього бою. Стрілецька зброя залишається ключовим інструментом тактичних операцій, але її ефективність залежить від відповідності конструктивних характеристик, ергономічності та підготовки особового складу до складних умов міських операцій. Актуальність дослідження зумовлена трансформацією характеру сучасних війн, де міські території стають основним театром бойових дій через їх стратегічне значення. Бої в містах ускладнюються обмеженою видимістю, високим ризиком рикошетів, акустичними викривленнями та необхідністю уникати побічної шкоди цивільному населенню. Традиційні методи підготовки та оцінювання стрілецької зброї, орієнтовані на відкриту місцевість, не повною мірою відповідають вимогам урбаністичного бою, що потребує нових підходів до тренувань і тестування озброєння.

Аналіз останніх досліджень і публікацій. Останнє десятиліття характеризується зростанням уваги науковців до питань підготовки військовослужбовців до ведення бойових дій у містах. У роботах [1], [10] зазначено, що міський бій має унікальні характеристики, які

потребують принципово нового підходу до організації тактичної підготовки, логістики та застосування стрілецької зброї. Традиційні методики стають менш ефективними в умовах складної забудови, обмеженої просторової доступності й посиленого ризику цивільних втрат. Дослідження [4], [17] наголошують на необхідності врахування специфіки багатоповерхового простору, низької видимості, великої кількості природних укриттів та щільної забудови під час планування операцій. В роботі [12] додатково підтверджено, що успішність стрільця у місті залежить не лише від технічних параметрів зброї, а й від рівня автоматизації дій, досягнутого завдяки спеціалізованому тренуванню.

Увагу науковців привернула також проблема адаптації стрілецької зброї до урбаністичного середовища. Так, в дослідженнях [2], [16] увага сконцентрована на питанні зменшення габаритів і маси зброї, покращення її ергономіки, а також зниження ризиків, пов'язаних із рикошетами в замкнутих приміщеннях. Разом з тим, більшість існуючих методик тестування озброєння розроблені для полігонів з відкритим простором і не враховують специфіки міських боїв. В окремих дослідженнях, зокрема [8], аналізується ефективність використання віртуальних тренажерів для підвищення навичок стрільців. Проте моделювання міських сценаріїв у таких системах часто відрізняється фрагментарністю і недостатньою відповідністю реальним бойовим умовам. Незважаючи на значний обсяг наукових публікацій, наразі відчувається нестача комплексних підходів, які б інтегрували оцінку ефективності стрілецької зброї в умовах міста з практичними аспектами її використання та методами тактичної підготовки особового складу.

Метою статі є: проведення обґрунтування методологічних основ оцінки ефективності стрілецької зброї та підготовки особового складу для ведення бойових дій в урбанізованих умовах.

Виклад основного матеріалу. У сучасних збройних конфліктах, особливо з урахуванням трансформації характеру ведення бойових дій, значно зростає роль урбанізованого середовища як домінуючого театру воєнних операцій, де стрілецька зброя залишається основним інструментом збройного протистояння на тактичному рівні. Насамперед урбанізоване середовище характеризується високим ступенем структурної складності, що виражається у щільному розташуванні багатоповерхової забудови, наявності вузьких вуличок, внутрішніх двориків, підземних комунікацій, мостів, арок, барикад, руїн та інших архітектурних об'єктів, які створюють хаотичну, фрагментовану і багаторівневу бойову обстановку. Таке середовище суттєво обмежує пряму видимість, зменшує діапазон маневру, знижує ефективність важкої техніки, проте водночас створює численні можливості для раптових атак, засідок, маневру малими групами й снайперської стрільби. У цій ситуації особливо важливо оцінювати не лише технічні характеристики стрілецької зброї: калібр, дальність пострілу, пробивну здатність чи скорострільність, але і її ергономічність, здатність до швидкої зміни позиції стрільця, ефективність стрільби у замкнутих просторах, а також вплив оточуючого середовища на траєкторію кулі та безпеку для союзників.

Фізико-геометричні особливості міських територій зумовлюють значне обмеження можливості ведення прицільного вогню на довгі дистанції. Більшість контактів із супротивником у міських умовах відбувається на дистанціях до 100 метрів, приблизно в межах 20-50 метрів, що передбачає домінування ближнього бою. Таким чином, довжина вулиць, ширина проходів, висота забудови, наявність численних кутів і перегородок формують мозаїчний простір, у якому стрілець повинен адаптуватися до раптових змін напрямку загрози. Перевага тут надається короткоствольній зброї або зразкам зі складними прикладами, зменшеними габаритами, високою точністю коротких черг. Крім того, вертикальна компонента простору: дахові поверхи, вікна, підвальні приміщення та вимагає урахування тривимірності бойової ситуації, що вказує на те, що стрілецька зброя має давати беззбійну стабільну вогневу реакцію на різних рівнях, як зверху вниз, так і знизу вгору та горизонтально [14].

Одним з викликів застосування стрілецької зброї в урбанізованому середовищі є обмежений простір, який не лише ускладнює вільне пересування, але й зменшує

маневреність стрільця, особливо при зміні позицій або відкатів під вогнем. У замкнених просторах: сходові клітки, вузькі коридори, кімнати, коли стрілецька зброя великого розміру (наприклад автоматичні гвинтівки) може стати перешкодою для ефективного реагування на загрозу. Ситуація ускладнюється тим, що бої в таких умовах зазвичай відбуваються у формі ближніх контактів, що не дає часу на прицілювання, вимагаючи від зброї не лише зручності, але й високої надійності при інтенсивному використанні. З цієї причини, збройні сили багатьох країн світу впроваджують спеціалізовані штурмові варіанти гвинтівок, карабіни, пістолети-кулемети або навіть гладкоствольну зброю з бойовими набоями для ведення бою в закритих приміщеннях.

Окремо зазначаємо, що стрільба в умовах міського середовища супроводжується специфічними акустичними характеристиками, які суттєво впливають як на психологічний стан військовослужбовців, так і на оперативну обстановку. Вузькі вулиці, бетонні фасади, скляні поверхні створюють ефект багатократного відлуння, яке не лише спотворює напрямок джерела пострілу, але й ускладнює комунікацію між підрозділами. Звукове перевантаження може дезорієнтувати бійця, унеможливаючи швидке реагування на загрози та порушуючи координацію вогневих дій. У таких умовах особливу роль відіграють глушники, які не тільки знижують чутність пострілу, але й зменшують ймовірність виявлення позиції стрільця. Проте слід і врахувати той факт, що використання глушників іноді знижує пробивну здатність кулі, тому рішення про їх застосування повинне базуватися на конкретному тактичному сценарії [1].

Ще однією специфікою міського бою є високий ризик рикошетів, що обумовлений наявністю твердих поверхонь, як то бетонних стін, металевих конструкцій, асфальтових покриттів, які сприяють зміні траєкторії кулі після удару. В товщі щільної забудови кулі, особливо якщо стрільба ведеться під кутом або всередині приміщення, можуть рикошетити та становити загрозу як для союзників, так і для цивільного населення, що є причиною додаткових викликів до вибору типу боєприпасів: зокрема, застосування набоїв з розширювальними кулями або зниженою рикошетною здібністю характеристиками є доцільним у приміщеннях з відбиваючими поверхнями. Не менш важливим є фактор того, що стрілець, який діє в урбаністичному середовищі, повинен володіти специфічною підготовкою, що включає не лише стрільбу у звичних умовах полігону, а й моделювання сценаріїв ведення вогню у приміщеннях, багаторівневих структурах, з вікон і дверей, із рухомих платформ. З цих причин урбанізоване середовище виступає не тільки як фон бойових дій, а й активним фактором, що визначає специфіку застосування стрілецької зброї і воно формує особливі вимоги до її конструкції, габаритів, калібру, пробивної здатності, акустичних характеристик та стійкості до рикошетів. У поєднанні з обмеженим простором, багаторівневистістю простору, нестабільністю оперативної обстановки та високою щільністю забудови, міські умови вимагають перегляду традиційних методів оцінювання ефективності стрілецької зброї та підходів до бойової підготовки персоналу [11].

На відміну від умов відкритого простору, міське середовище вносить суттєві корективи як до параметрів застосування вогнепальної зброї, так і до вимог щодо її конструктивних, функціональних і тактико-технічних характеристик, що чітко визначає необхідність критичного осмислення існуючих критеріїв оцінювання та розробки нових методичних підходів, які б повною мірою враховували специфіку урбаністичного бою. Оцінювання ефективності стрілецької зброї в урбанізованому середовищі має спиратися на комплексний підхід, який враховує не лише суто технічні показники зброї, а й оперативно-тактичні, ергономічні, психологічні та просторово-функціональні аспекти її застосування. Одним з критеріїв оцінки виділяємо точність стрільби, яка визначає ймовірність ураження цілі з першого пострілу, особливо в умовах обмеженої видимості, коротких дистанцій і великої кількості перешкод. Висока точність забезпечує мінімізацію боєприпасів, зменшує побічну шкоду та підвищує ефективність дій у щільній забудові, де навіть один промах може спричинити рикошет або ненавмисне ураження цивільних осіб [16].

Наступним критерієм для оцінки є пробивна здатність, яка в умовах міського бою набуває особливого значення через потребу уражати супротивника за різними бар'єрами – бетонними, цегляними, дерев'яними чи металевими – які слугують природними або створеними укриттями. Залежно від типу перешкод, відстані та кута влучання, зброя повинна забезпечувати достатню кінетичну енергію кулі для подолання захисту та ураження цілі, водночас не створюючи надмірної загрози для третьої сторони за межами цільового простору. Саме тому методики оцінки мають включати випробування стрілецької зброї на різних типах будівельних матеріалів, що моделюють стіни, двері, віконні рами та інші типові елементи інфраструктури.

Також робимо наголос і на ергономічність зброї, що охоплює її масогабаритні характеристики, зручність утримання, баланс, розташування елементів управління та легкість перезаряджання. У замкнених просторах, зокрема коридорах, сходових клітках, кімнатах та переходах, значення ергономічності зростає в геометричній прогресії, оскільки вона визначає, наскільки стрілець здатен ефективно діяти у стиснутому просторі, уникати затримок при зміні позицій та мінімізувати час на приведення зброї в бойовий стан. Маємо окреслити і критерій зручності застосування зброї в замкнених просторах, де поєднання геометричної складності, акустичних викривлень, освітлювальних контрастів і психологічного навантаження створює унікальне середовище, яке суттєво впливає на здатність стрільця діяти швидко, точно і з мінімальним ризиком для себе та інших. Методична оцінка такої характеристики повинна базуватись на принципі адаптивності: наскільки зброя дозволяє швидко реагувати на появу цілі, наскільки легко нею оперувати в умовах обмеженої рухливості, чи забезпечується достатня стабільність при стрільбі в нестандартних положеннях. Також до уваги слід брати фактор наявності або відсутності додаткових пристроїв: глушників, підствольних ліхтарів, коліматорних прицілів, які можуть впливати як на ефективність ураження, так і на загальну ергономіку комплексу [3].

Перспективним напрямком сучасної методики оцінювання ми визначаємо використання адаптованих полігонів та тренажерних комплексів, які відтворюють характерні елементи міського середовища і дозволяють апробувати зброю в умовах, максимально наближених до реальних. Такі полігони повинні бути побудовані з урахуванням структурної складності міської забудови, включати кімнати різного типу, сходові марші, арки, вузькі коридори, місця з різким освітленням, вікна, двері, підвали тощо [6]. Крім того, полігони можуть оснащуватися електронними цілями, які реагують на влучання, і акустичними системами, що моделюють реалістичне звукове середовище бою (відлуння, постріли, крики, сигнали), забезпечуючи повноцінну сенсорну стимуляцію (табл. 1).

Високий потенціал мають також віртуальні тренажери і доповнена реальність (AR/VR), які дозволяють не лише імітувати бойову обстановку без фізичного ризику, але й забезпечують високу варіативність сценаріїв, зберігаючи об'єктивність оцінки параметрів ефективності. Наприклад, VR-середовище може точно моделювати конфігурацію бойового простору, включаючи положення перешкод, розташування супротивника, динамічні зміни ситуації, погодні умови, нічний режим, а також відстежувати рухи стрільця, якість прицілювання, тривалість реакції, стабільність зброї при різних положеннях тіла. У поєднанні з біометричними сенсорами такі системи дають змогу проводити оцінку не лише технічної, але й психологічної готовності до застосування зброї у стресових умовах міського бою (рис. 1).

Таблиця 1

Оцінювання ефективності використання стрілецької зброї в урбанізованому середовищі
(сформовано автором)

Критерій оцінки	Опис	Метод оцінки	Умови тестування	Очікуваний результат	Вага критерію (%)
Точність стрільби	Ймовірність ураження цілі з першого пострілу в умовах обмеженої видимості, коротких дистанцій та перешкод	Випробування на статичних і динамічних мішенях, стрільба з різних положень (стоячи, з коліна, лежачи, з-за укриття)	Обмежена видимість, змінне освітлення, дистанція 5-50 м, наявність перешкод (стіни, меблі)	Ураження цілі з першого пострілу у $\geq 85\%$ випадків	30
Пробивна здатність	Здатність кулі пробивати типові міські бар'єри (бетон, цегла, дерево, метал) без надмірної побічної шкоди	Тестування на будівельних матеріалах (стіни 10-30 см, двері, віконні рами) з різними кутами влучання	Дистанція 10-100 м, кути влучання 0° - 45° , різні типи боєприпасів	Пробиття бар'єра з ураженням цілі за ним у $\geq 80\%$ випадків	25
Ергономічність	Зручність утримання, баланс, легкість перезаряджання, компактність у замкнених просторах	Симуляція бою в обмеженому просторі (коридори, сходи, кімнати), тестування перезаряджання та маневрування	Вузькі простори (ширина 0.8-1.5 м), стрільба з однієї руки, з плеча, лежачи	Час приведення зброї в бойовий стан ≤ 2 с, комфортність $\geq 90\%$ за оцінкою стрільців	20
Зручність застосування в замкнених просторах	Адаптивність до швидкої реакції, стабільність при стрільбі в нестандартних положеннях, вплив додаткових пристроїв	Тестування на адаптованих полігонах з імітацією міських умов, оцінка швидкості прицілювання	Обмежений простір, змінне освітлення, наявність глушників/прицілів, динамічні цілі	Час реакції на ціль ≤ 1.5 с, стабільність прицілювання $\geq 80\%$	15
Ефективність у бойових сценаріях	Здатність зброї забезпечувати виконання тактичних завдань у реальних міських умовах	Моделювання сценаріїв (штурм, зачистка, оборона) на полігонах та у VR/AR-тренажерах	Багаторівневий простір, рухомі цілі, стрес-фактори (шум, відлуння, обмежений час)	Успішне виконання завдання у $\geq 90\%$ сценаріїв, збереження $\geq 50\%$ боєприпасів	1



Рисунок 1 – Віртуальний тренажер з телеметричною розміткою для підготовки стрільця в умовах міського бою [15]

Враховуються і можливості інтегрованих систем оцінки, які поєднують результати полігонного, ситуаційного та симуляційного тестування, дозволяючи формувати загальну рейтингову матрицю ефективності різних зразків зброї у специфічних умовах урбанізованого середовища. Такі системи дозволяють зіставляти різні моделі за сукупністю критеріїв – точність, пробивна здатність, ергономічність, швидкість реагування, безпечність, модульність, стійкість до впливу факторів середовища і приймати обґрунтовані рішення щодо їхньої доцільності для озброєння конкретних підрозділів [13]. У реальних умовах ведення бойових дій в урбанізованому середовищі стрілець, який перебуває за укриттям і готується до відкриття вогню, не завжди має можливість точно визначити кількість противників, оскільки частина з них може залишатися прихованою за архітектурними елементами приміщення або з'явитися лише безпосередньо в ході бойового контакту. Саме тому одним із ключових завдань є мінімізація відкритої площі власного тіла, видимої противнику під час візуального спостереження чи прицілювання, що вимагає не лише правильного вибору позиції, а й вміння швидко адаптуватися до просторових обмежень (рис. 2).



Рисунок. 2. – Варіанти бойових стійок стрільця під час ведення вогню з-за укриття в урбанізованому середовищі [8]

Стрільба з-за укриття передбачає особливу бойову стійку, що суттєво відрізняється від класичної, з урахуванням необхідності забезпечити максимально можливий захист стрільця від вогню супротивника. Залежно від типу укриття – стіна, дверний отвір, вікно, барикада, транспортний засіб – вибирається відповідне положення для стрільби: стоячи, з коліна, лежачи або в інших нестандартних варіантах, включаючи стрільбу з положення лежачи на боці чи з однієї руки. Під час бойової підготовки необхідно моделювати переміщення між

різними типами укриттів, відпрацьовуючи не лише стрільбу, а й логіку зміни позиції, швидкість реагування та оцінку обстановки в динаміці [5].

Для контролю правильності занять укриття рекомендується використовувати методичні засоби, зокрема великі дзеркала, що встановлюються перед укриттям, аби стрілець мав можливість побачити частину власного силуету, яка залишається відкритою з точки зору умовного супротивника. Такий прийом – це джерело наочного усвідомлення помилки позиціювання, скоригувати нахил корпусу, розташування рук і зброї, а також удосконалити техніку скорочення вразливої площі тіла під час стрільби (рис. 3.).



Рисунок 3 – Імітація бойового положення стрільця за укриттям з використанням дзеркального контролю силуету [8]

Сама тактика відкриття вогню з укриття тісно пов'язана з динамікою бойових дій у міських умовах, де виявлення загрози часто супроводжується раптовим і стрімким переміщенням до найближчого безпечного об'єкта. У таких ситуаціях стрілець може бути змушений вести вогонь як під час руху до укриття, так і безпосередньо з-за нього, що вимагає вже від стрілка високого рівня автоматизму, що формується лише в результаті системного багаторазового тренування. Зокрема, необхідно навчитися в короткий проміжок часу виконувати комплекс послідовних дій: швидко оцінювати обстановку (визначати кількість супротивників, рівень їхньої озброєності та ймовірні наміри), приймати рішення щодо доцільності відкриття вогню на місці або після зайняття укриття, визначати найближчий придатний об'єкт для укриття, ще під час руху планувати положення для стрільби, а також тримати в полі зору пересування супротивника з метою передбачення його дій.

У процесі навчання на полігоні або в спеціалізованих тирах, стрілець не повинен заздалегідь знати, по яких саме мішенях йому доведеться відкривати вогонь. Цільові об'єкти встановлюються на різних відстанях та в різних просторових конфігураціях, що відображає складність і непередбачуваність бойових ситуацій і певна частина мішеней може імітувати збройного противника, частина – незброєних осіб або умовних заручників, що вимагає від стрільця негайного тактичного аналізу й обґрунтованого прийняття рішення: відкривати вогонь одразу, переміщуватися до укриття або взагалі утриматися від пострілу, щоб уникнути помилкового ураження (рис. 4.).

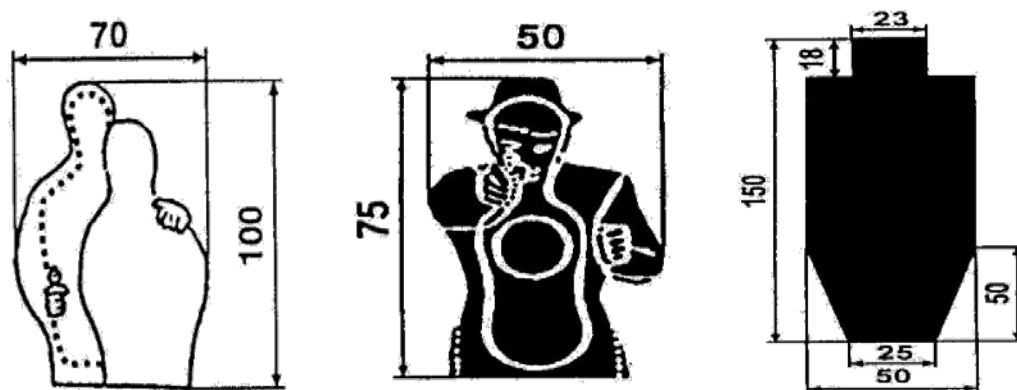


Рисунок 4 – Схематичні зображення навчальних мішеней для моделювання бойових ситуацій в урбанізованому середовищі [7]

У деяких вправах доцільно включати дзеркальну роботу, так звану «стрільбу вхолосту» по власному відображенню, яке виконує роль імітації противника, що веде вогонь з-за укриття. Такий підхід дозволяє тренувати не лише стрільбу як технічну дію, але й просторову орієнтацію, оцінку видимості, положення корпусу, силу натискання на спусковий гачок і баланс тіла. Згадані прийоми та вправи мають бути інтегровані до програми підготовки за дисциплінами, що стосуються вогневої підготовки і тактики особистої безпеки військовослужбовця. Їхня методологічна база повинна включати адаптивні сценарії бойового застосування зброї у міському середовищі, де пріоритет надається не стільки формальній точності стрільби, скільки здатності ефективно діяти у змінному тактичному середовищі. Переважна частина бойових зіткнень в міському середовищі відбувається саме в закритих просторах, таких як житлові будівлі, адміністративні споруди, підземні об'єкти та багаторівневі інфраструктурні вузли, де безпосередній контакт із противником часто зводиться до стрілецької перестрілки на відстані кількох метрів або навіть у межах однієї кімнати. Такий характер бою зумовлює крайню швидкоплинність подій: бойове зіткнення може спалахнути зненацька й завершитися впродовж кількох секунд, що ставить надзвичайно високі вимоги до рівня підготовки особового складу та до можливостей стрілецької зброї ефективно застосовуватись у критично обмеженому просторі [7].

В основі успішності дій підрозділів у закритих урбанізованих просторах лежить здатність особового складу діяти узгоджено, миттєво приймати тактичні рішення та використовувати стрілецьку зброю з високим ступенем автоматизму, що формується винятково завдяки системному тренуванню. Значна складність таких умов пов'язана з постійним ризиком змішування комбатантів і неозброєного цивільного населення, що унеможливорює беззастережне застосування вогню та вимагає від кожного бійця високого рівня ситуаційного аналізу та вибіркової реакції. Бойові дії у вузьких коридорах, сходових маршах або кімнатах повинні плануватися з особливою ретельністю, а виконуватися з точністю на рівні кожної вогневої групи. Навчання повинне бути структуровано таким чином, аби кожен військовослужбовець розумів свої функції в контексті дій цілого підрозділу, а також володів основами тактики ведення бою в замкнутих приміщеннях. Зокрема, слід враховувати три основні принципи, що визначають тактику штурму: раптовість, швидкість і контрольована агресія [10].

Раптовість у бойових діях у межах будівель є визначальним чинником, який дозволяє отримати тимчасову перевагу навіть над чисельно переважаючим супротивником. Її досягають шляхом раптового проникнення, введення супротивника в оману, використання спеціальних засобів (як-от світлошумові гранати) або ж завдяки ретельно спланованій зміні напрямку атаки. При цьому потрібно враховувати, що ефективність таких методів залежить від ступеня підготовки ворога: необізнаний супротивник втрачає орієнтацію, тоді як досвідчений боець може миттєво адаптуватися до ситуації.

Швидкість дій – це критичний аспект безпеки штурмової групи. Висока динаміка входу в приміщення, переміщення між секторами та нейтралізація загроз дозволяє скористатися ефектом раптовості й не дати ворогу часу на реакцію. Проте така швидкість має бути скоординованою, не хаотичною, що знову ж таки підкреслює важливість належної підготовки. Контрольована агресія означає необхідність швидкого та рішучого ураження противника при водночас повному контролі над бойовою ситуацією, із запобіганням надмірному застосуванню сили, особливо в контексті можливості присутності цивільних осіб або заручників. Така агресія не обмежується лише вогневим ураженням, вона передбачає психологічну перевагу, домінування у приміщенні та примус ворога до капітуляції або нейтралізації [11]. Уваги потребує і адаптація техніки стрільби до умов ближнього бою. Під впливом сильного стресу, спричиненого безпосередньою загрозою життю, у людини активізуються фізіологічні реакції, що знижують точність тонких моторних дій і зменшують когнітивні здібності. Саме тому класичні позиції стрільби стають малоефективними або навіть небезпечними. У таких умовах доцільно використовувати максимально прості, природні положення для стрільби, які легко відтворити на рівні м'язової пам'яті, навіть у стані бойового стресу [15]. Як правило, стрільба ведеться подвійними пострілами або короткими чергами, оскільки більш тривала стрільба ускладнює контроль над прицільною лінією, що особливо критично у закритих приміщеннях. Також необхідно враховувати правила тактичної перезарядки: магазин змінюється до повного вичерпання, аби уникнути ситуації, коли стрілець вступає в новий контакт із неповним боєкомплектom. При цьому частково використаний магазин зберігається для подальшого застосування (табл. 2).

Таблиця 2

Тактика ведення бойових дій в обмеженому міському просторі (сформовано автором)

Аспект тактики	Характеристика	Спосіб виконання	Умови застосування	Очікуваний ефект	Значимість (%)
Маневреність групи	Здатність швидко пересуватися в обмеженому просторі	Координоване переміщення парами, використання кутів і укриттів	Вузькі коридори, дверні отвори, сходи; дистанція 1-10 м	Просування без втрат за ≤ 15 с на 10 м	25
Тактична координація	Синхронізація дій між бійцями штурмової групи	Попередній розподіл зон відповідальності, сигнальна комунікація	Закриті приміщення, обмежена видимість, шумове тло	Успішна зачистка сектора у $\geq 90\%$ випадків	20
Контроль зони	Забезпечення домінування в приміщенні	Постійне спостереження за секторами, прикриття флангів	Кімнати, переходи, багаторівневі структури	Повний контроль зони за ≤ 20 с	20
Ефективність вогню	Точне ураження цілей в умовах ближнього бою	Стрільба короткими чергами, використання коліматорних прицілів	Дистанція 1-15 м, динамічні цілі, обмежений простір	Ураження цілі з ≤ 2 пострілів у $\geq 85\%$ випадків	20
Управління стресом	Збереження боєздатності в умовах психологічного тиску	Тренування м'язової пам'яті, спрощені пози стрільби	Високий рівень шуму, раптові загрози, стиснутий простір	Збереження точності стрільби $\geq 75\%$ під тиском	15

Переміщення всередині приміщень має відбуватися чітко, швидко, з мінімальними звуковими та візуальними проявами. Забороняється повертати голову окремо від тіла і вся система зброя→руки→торс повинна рухатися єдиним блоком, що дозволяє зберігати рівновагу, не перевантажуючи спину та ноги, а також миттєво наводити зброю у напрямку загрози. Тримання зброї на витягнутих руках і не лише технічний прийом, а й фізіологічна реакція на стрес, що дозволяє стріляти інтуїтивно в точку, на яку спрямований погляд. Цінним тактичним компонентом є взаємне прикриття під час пересування, особливо в таких зонах як сходи, перехрестя коридорів, дверні отвори чи інші відкриті простори, де можливе

раптове виявлення супротивника. Саме тому штурмова група повинна мати чітку структуру. Базовою одиницею є пара стрільців, які забезпечують один одного у бою. Повна штурмова група складається, зазвичай, із чотирьох-шести осіб і працює у двох елементах, які чергують дії, коли один здійснює зачистку, інший прикриває.

При русі стрілок тримає зброю навідною у напрямку просування, приклад притиснутий до плеча, ствол дещо опущений, аби не звужувати кут огляду. Обидва ока залишаються відкритими для кращого контролю простору. Надзвичайно важливо уникати зайвих рухів зброєю, особливо в місцях з обмеженою оглядовістю, щоб не демаскувати себе і не створити ризик захоплення зброї. Зброя має перебувати на запобіжнику до моменту ідентифікації загрози. Завершивши зачистку сектора, стрілець повертає зброю в безпечний стан. У випадку затримки при стрільбі чи іншої несправності, боєць негайно присідає на одне коліно, усуває несправність, і лише після стабілізації ситуації повертається до бою. Це дозволяє іншим учасникам групи миттєво зрозуміти, що сектор потребує перекриття, і забезпечити взаємну підтримку [9].

Першим кроком у системі випробувань є етап підготовки, що передбачає аналіз технічної документації на зразок зброї, визначення завдань випробування та формування випробувального середовища, яке максимально імітує умови реального міста. На цьому етапі розробляються сценарії, що включають стрільбу в умовах обмеженої видимості, стрільбу з-за укриттів, з кімнат, коридорів, вікон, сходових майданчиків, а також враховуються можливості для динамічного маневрування. Крім того, створюється відповідна інфраструктура: мішеневі установки, захисні бар'єри, акустичні сенсори, фіксатори траєкторії куль та відеореєстратори, що дозволяють детально аналізувати результати.

Другим і найбільш ресурсно-інтенсивним є етап проведення випробувань, під час якого здійснюється перевірка таких ключових параметрів, як точність стрільби на різних дистанціях (особливо в межах 10–50 м, які є критичними для бою в місті), швидкість приведення зброї до бою, надійність при стрільбі в складних просторових конфігураціях (з нестандартних положень, у русі, з-за бар'єрів), стійкість до рикошетів, акустична непомітність (при використанні глушників), а також ергономічність і зручність при переході між різними бойовими позиціями. До випробувань залучаються інструктори, військовослужбовці, а також фахівці з тактики ближнього бою, що дозволяє поєднати технічну та практичну оцінку зброї [2]. Прискіпливе відношення на цьому етапі до перевірки адаптивності зброї до змінних умов бою, зокрема зміні освітлення, шумовому навантаженню, дії під час обмеженої оглядовості, переходу зі світлих зон у темні приміщення та навпаки. Випробування передбачають моделювання стрілецьких ситуацій в умовах багатоповерхової забудови, включаючи стрільбу по цілях, що з'являються несподівано, або тих, що знаходяться за напівпрозорими або легкими укриттями. Оцінюється не лише технічна ефективність зброї, а й можливість її швидкої розрядки, перезарядки, збереження лінії прицілювання при зміні положення тіла стрільця.

Третім обов'язковим етапом є фіксація результатів випробування, яка виконується за допомогою інтегрованих електронних систем збору та обробки даних, коли включені фото- та відеофіксація дій стрільця, контроль за влучанням, хронометраж стрільби, облік кількості пострілів до ураження цілі, а також оцінку зусиль при утриманні зброї у прицільному положенні протягом заданого часу. На цьому етапі здійснюється порівняння фактичних характеристик зразків зі стандартами та нормативами, проводиться балістичний аналіз, оцінюється ступінь втомлюваності стрільця та відповідність конструкції зброї умовам бойового застосування в місті [4]. У процесі бойового застосування стрілецької зброї в умовах міських боїв, численні приклади з реальних операцій підтверджують, що успішність бойових дій у великій мірі залежить від відповідності зброї тактичному сценарію. Зокрема, досвід сучасної війни в Україні засвідчив доцільність використання зброї компактного типу – таких як автоматичні карабіни короткого формату, пістолети-кулемети (наприклад, MP5), та модульні автоматичні гвинтівки (на кшталт FN SCAR або CZ BREN 2), які дозволяють ефективно вести вогонь у закритих приміщеннях. Високу оцінку в бойових умовах отримала

також зброя з можливістю встановлення коліimatorних або голографічних прицілів, які забезпечують точне прицілювання в умовах обмеженого часу на реакцію.

Міжнародний бойовий досвід, наприклад у контексті операцій НАТО в Афганістані чи в ході міських бойових дій на Близькому Сході, свідчить про те, що перевага надається зброї з покращеною маневреністю, зокрема штурмовим гвинтівкам з укороченим стволом, пістолетам-кулеметам зі зниженою масою, а також автоматичній зброї з низькою віддачею, що дозволяє вести точну стрільбу чергами навіть у нестабільному положенні. В умовах тісної забудови застосування глушників та спеціальних боєприпасів також є важливим фактором для зменшення демаскування стрільця та зниження ризику рикошетів. У результаті проведення випробувань на полігонах, адаптованих до міських умов, сформовано рекомендований перелік зразків стрілецької зброї, що демонструють високу ефективність у міських бойових діях. До них, зокрема, належать [5; 8]:

- HK416 і HK417 – універсальні штурмові гвинтівки з високою надійністю, адаптовані до динамічного бою та широкої модульності;

- FN SCAR-L – компактна, точна та зручна в управлінні зброя для роботи в замкнутих просторах;

- B&T APC9 – пістолет-кулемет, що поєднує малу віддачу з високою швидкістю влучного вогню;

- AR-15 короткого формату – платформи з можливістю індивідуального налаштування, які довели свою ефективність у зачистках приміщень;

- українські модернізовані версії АК-74 (наприклад, «Малюк») – завдяки булпап-конструкції мають компактні габарити при збереженні довжини ствола, що особливо доречно у вузьких коридорах.

Усі перелічені зразки повинні оцінюватися не лише за балістичними характеристиками, але й за параметрами сумісності з екіпіруванням, адаптивністю до швидкої зміни бойових умов, зручністю експлуатації в бронежилеті, у протигазі чи з додатковими захисними елементами, а також за ступенем інтуїтивної керованості у стані бойового стресу. Отже, випробування стрілецької зброї для міських умов не може зводитися виключно до формального тестування її технічних параметрів. Йдеться про необхідність формування цілісної методики, що інтегрує тактичне моделювання, аналітичну обробку даних, порівняльне оцінювання і бойове апробування.

Висновки. Було проаналізовано ключові чинники, що суттєво впливають на результативність застосування стрілецької зброї в міських умовах. До них належать складна архітектурна структура забудови, обмеженість простору для тактичного маневру, часта необхідність змінювати рівень прицілювання, висока концентрація перешкод, велика ймовірність рикошетів, а також специфічні акустичні та психологічні навантаження, характерні для бойових дій у місті. Розроблено комплексну систему критеріїв для оцінки ефективності стрілецької зброї, яка передбачає багаторівневе тестування, коли система враховує фізичні характеристики зброї, тактичні параметри її використання, а також психологічний стан оператора. У процесі тестування передбачено проведення випробувань на спеціально адаптованих полігонах, моделювання реальних бойових ситуацій із використанням технологій віртуальної та доповненої реальності (VR/AR), аналіз вогню з нетипових положень, а також оцінку поведінки стрільця в умовах сильного стресу.

Докладно вивчено особливості тактики штурмових операцій у густо забудованих районах. Встановлено, що успішність таких дій значною мірою залежить від раптовості, швидкості реакції, а також контролю над застосуванням силового тиску. Ефективність вогню в урбаністичному середовищі визначається не лише технічною точністю зброї, а й ступенем автоматизму дій стрільця, його здатністю швидко адаптуватися до змін у ситуації, координувати взаємодію в складі штурмової групи та оперативно приймати рішення щодо початку чи припинення вогню. Запропоновано ряд методичних прийомів для підвищення ефективності підготовки: стрільба по рухомих цілях у вузьких просторах, використання дзеркал для контролю положення тіла під час зайняття позиції, моделювання раптової

загрози з боку мирного населення, класифікація цілей за рівнем небезпеки, а також тренування в умовах нестандартного освітлення. Доведено, що тільки комплексне впровадження цих елементів у навчальні курси забезпечує стійке засвоєння навичок, необхідних для ефективних дій у міському просторі. Запропоновано створити трирівневу модель випробувань стрілецької зброї: 1) Аналітико-планувальний етап, спрямований на визначення умов, параметрів та цілей випробувань; 2) практичний етап, що передбачає виконання стрільб у різноманітних конфігураціях урбаністичного середовища з використанням систем об'єктивного контролю; 3) етап аналізу результатів, який дає змогу узагальнити отримані дані, провести порівняльну оцінку та сформулювати рекомендації для військових підрозділів щодо вибору оптимальних зразків зброї.

ЛІТЕРАТУРА:

1. Військові операції на урбанізованій місцевості (MOUT). Бойовий статут морської піхоти США (MCWP) 3-35.3. Київ: Вид. «КНТ», 2023. 405 с.
2. Зеленський Є. С., Задорожня Р. В., Фісун Н. О. Використання інтерактивних методів навчання під час проведення практичних занять з вогневої підготовки. Науковий вісник Ужгородського національного університету. Серія: Право. 2023. Вип. 80. ч. 2. С. 144-148. DOI: <https://doi.org/10.24144/2307-3322.2023.80.2.21>.
3. Конєв О. Ю., Геращенко О. С. Удосконалення методики навчання вогневої підготовки здобувачів вищої освіти навчальних закладів зі специфічними умовами навчання та цивільних осіб в умовах воєнного стану. Південноукраїнський правничий часопис. 2022. № 1-2. С. 99-104. DOI: <https://doi.org/10.32850/sulj.2022.1-2.18>
4. Кучерина С. Є., Гриненко С. О., Олейніков Д. О. Організаційно-правові засади застосування і використання співробітниками Служби безпеки України вогнепальної зброї, спеціальних засобів та заходів фізичного впливу : монографія. Харків : Право, 2016. 136 с.
5. Наточій А. Д., Болгаренко В. М. Вогнева підготовка та формування професійних якостей у майбутніх офіцерів: взаємозв'язок та взаємозалежність. Аналітично-порівняльне правознавство. 2024. № 3. С. 64-72. DOI: <https://doi.org/10.24144/2788-6018.2024.03.64>
6. Самсонов Ю. В., Радіонов Г. О., Белашов Ю. О., Пурнак В. П., Бірук А. І. Сутнісні характеристики формування готовності рекрутів Національної гвардії України до застосування стрілецької зброї в екстремальних умовах службово-бойової діяльності. Інноваційна педагогіка. 2024. № 77. С. 177–184. DOI: <https://doi.org/10.32782/2663-6085/2024/77.36>
7. Сучасні види вогнепальної стрілецької зброї підрозділів МВС України : навчальний посібник / Ю. Р. Йосипів, В. М. Синенький, М. Д. Курляк, М. О. Лиса, Н. Д. Туз, П. С. Вербицький, за заг. ред. Ю. Р. Йосипіва. Львів: Львівський державний університет внутрішніх справ, 2022. 184 с.
8. Хацаюк О., Самсонов Ю., Самсонова Г. Підготовка інструкторів з вогневої підготовки : колект. моногр. London-Chisinau : Dodo Books Indian Ocean Ltd. and OmniScriptum S.R.L. publishing group, 2024. 81 с.
9. Akintayo J., Romaniuk S. Small Arms and Light Weapons. In: The Palgrave Encyclopedia of Global Security Studies, edited by S. Romaniuk & P. Marton. Palgrave Macmillan. 2022. pp. 1340–1343. DOI: [10.1007/978-3-319-74336-3_128-1](https://doi.org/10.1007/978-3-319-74336-3_128-1)
10. Coleman J. L., Davey P., McClelland J. A., Middleton K. J. The use of small-arms stability measures in combat shooting assessments. Applied Ergonomics. 2025. Vol. 122, Article 104385. DOI: [10.1016/j.apergo.2024.104385](https://doi.org/10.1016/j.apergo.2024.104385)
11. Handbook of Best Practice Guides on National Controls over the Manufacture of Small Arms and Light Weapons. Forum for Security Co-operation, Organization for Security and Co-operation in Europe (OSCE). Vienna, 1. December 2003. <https://www.osce.org/files/f/documents/e/a/13616.pdf>
12. Lang D., Zhou A. Relationships between postural balance, aiming technique and performance in elite rifle shooters. European Journal of Sport Science. 2022. Vol. 22. no 10. P. 1493–1498. DOI: [10.1080/17461391.2021.1971775](https://doi.org/10.1080/17461391.2021.1971775)
13. Makedon V., Myachin V., Plakhotnik O., Fisunen N., Mykhailenko O. Construction of a model for evaluating the efficiency of technology transfer process based on a fuzzy logic approach. Eastern-European Journal of Enterprise Technologies. 2024. no 2(13(128)). pp. 47-57. <https://doi.org/10.15587/1729-4061.2024.300796>.

14. Sarajevo Action Plan 2021–2024. Small Arms and Light Weapons (SALW) Control Strategy in Bosnia and Herzegovina and accompanying Action Plan. – Sarajevo : SEESAC, 2021. 44 p. DOI: 10.1017/S1816383110000366
15. Small Arms Survey. Statement for the Third Substantive Session of the Open-ended Working Group on Conventional Ammunition, 14 February 2023. Sarajevo: IANSA / Small Arms Survey, 2023. (Statement published FTS file). <https://iansa.org/wp-content/uploads/2023/01/Small-Arms-Survey-OEWG-3-Statement-14-Feb-2023-1.pdf>
16. Tsegaye D. A. The Impact of Proliferation of Small Arms on Human Security in Amhara Regional State, Ethiopia: The Case of Gondar City. Research paper presented in partial fulfillment of the requirements for the degree of Master of Arts in Development Studies. Ethiopia: Erasmus University Rotterdam, International Institute of Social Studies. 2024. <http://hdl.handle.net/2105/75737>
17. Vautravers A. Military operations in urban areas. International Review of the Red Cross. 2010. Vol. 92. no 878. P. 437–452. DOI: 10.1017/S1816383110000366

REFERENCES:

1. Viiskovi operatsii na urbanizovanii mistsevesti (MOUT). Boiovyi statut mors'koi pikhoty SShA (MCWP) 3-35.3 [Military operations in urban terrain (MOUT). US Marine Corps Combat Manual]. Kyiv: KNT, 2023. 405 p.
2. Zelenskyi Ye. S., Zadorozhnia R. V., Fisun N. O. (2023), “Vykorystannia interaktyvnykh metodiv navchannia pid chas provedennia praktychnykh zaniat' z vohnevoi pidhotovky” [Using interactive teaching methods during practical firearms training], Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Serii: Pravo, Issue 80, Part 2, pp. 144–148. DOI: <https://doi.org/10.24144/2307-3322.2023.80.2.21>.
3. Konev O. Yu., Herashchenko O. S. (2022), “Udoskonalennia metodyky navchannia vohnevoi pidhotovky zdobuvachiv vyshchoi osvity ta tsyvil'nykh osib v umovakh voiennoho stanu” [Improvement of firearms training methods for students and civilians in wartime], Pivdenoukrainskyi pravnychy chasopys, no. 1–2, pp. 99–104. DOI: <https://doi.org/10.32850/sulj.2022.1-2.18>.
4. Kucheryna S. Ye., Hrynenko S. O., Oleinykov D. O. (2016), Orhanizatsiino-pravovi zasady zastosuvannia i vykorystannia spivrobotnykamy Sluzhby bezpeky Ukrainy vohnepalnoi zbroi, spetsialnykh zasobiv ta zakhodiv fizychnoho vplyvu [Organizational and legal principles of using firearms and special means by the Security Service of Ukraine]. Kharkiv: Pravo, 136 p.
5. Natochii A. D., Bolhareno V. M. (2024), “Vohneva pidhotovka ta formuvannia profesiynykh yakosteï u maibutnykh ofitseriv: vzaïmozv'iazok ta vzaïmozalezhnist'” [Firearms training and development of professional qualities in future officers], Analitychno-porivnialne pravoznavstvo, no. 3, pp. 64–72. DOI: <https://doi.org/10.24144/2788-6018.2024.03.64>.
6. Samsonov Yu. V., Radionov H. O., Belashov Yu. O., Purnak V. P., Biruk A. I. (2024), “Sutnisni kharakterystyky formuvannia hotovnosti rekrutiv Natsionalnoi hvardii Ukrainy do zastosuvannia striletskoi zbroi” [Essential characteristics of NGU recruits' readiness to use firearms], Innovatsiina pedahohika, no. 77, pp. 177–184. DOI: <https://doi.org/10.32782/2663-6085/2024/77.36>.
7. Yosypiv Yu. R., Synenkyi V. M., Kurliak M. D., Lysa M. O., Tuz N. D., Verbytskyi P. S. (2022), Suchasni vydy vohnepalnoi striletskoi zbroi pidrozdiliv MVS Ukrainy [Modern types of firearms of the Ministry of Internal Affairs units]: Navch. posibnyk. Lviv: LDUVS, 184 p.
8. Khatsaiuk O., Samsonov Yu., Samsonova H. (2024), Pidhotovka instruktoriv z vohnevoi pidhotovky [Firearms instructor training]: Collective monograph. London–Chisinau: Dodo Books Indian Ocean Ltd. and OmniScriptum S.R.L. Publishing Group, 81 p.
9. Akintayo J., Romaniuk S. (2022), “Small Arms and Light Weapons”, in: The Palgrave Encyclopedia of Global Security Studies, edited by S. Romaniuk & P. Marton, Palgrave Macmillan, pp. 1340–1343. DOI: 10.1007/978-3-319-74336-3_128-1.
10. Coleman J. L., Davey P., McClelland J. A., Middleton K. J. (2025), “The use of small arms stability measures in combat shooting assessments”, Applied Ergonomics, vol. 122, Article 104385. DOI: 10.1016/j.apergo.2024.104385.
11. Forum for Security Co-operation, OSCE. (2003), Handbook of Best Practice Guides on National Controls over the Manufacture of Small Arms and Light Weapons. Vienna: OSCE. URL: <https://www.osce.org/files/f/documents/e/a/13616.pdf>.
12. Lang D., Zhou A. (2022), “Relationships between postural balance, aiming technique and performance in elite rifle shooters”, European Journal of Sport Science, vol. 22, no. 10, pp. 1493–1498. DOI: 10.1080/17461391.2021.1971775.

13. Makedon V., Myachin V., Plakhotnik O., Fisunen N., Mykhailenko O. (2024), "Construction of a model for evaluating the efficiency of technology transfer process based on a fuzzy logic approach", *Eastern-European Journal of Enterprise Technologies*, no. 2(13(128)), pp. 47–57. <https://doi.org/10.15587/1729-4061.2024.300796>.

14. SEESAC. (2021), *Sarajevo Action Plan 2021–2024. Small Arms and Light Weapons (SALW) Control Strategy in Bosnia and Herzegovina and accompanying Action Plan*. Sarajevo: SEESAC. 44 p.

15. Small Arms Survey. (2023), *Statement for the Third Substantive Session of the Open-ended Working Group on Conventional Ammunition*, 14 February 2023. Sarajevo: IANSA / Small Arms Survey. URL: <https://iansa.org/wp-content/uploads/2023/01/Small-Arms-Survey-OEWG-3-Statement-14-Feb-2023-1.pdf>.

16. Tsegaye D. A. (2024), *The Impact of Proliferation of Small Arms on Human Security in Amhara Regional State, Ethiopia: The Case of Gondar City*. Research paper for Master of Arts in Development Studies. Erasmus University Rotterdam, ISS. URL: <http://hdl.handle.net/2105/75737>.

17. Vautravers A. (2010), "Military operations in urban areas", *International Review of the Red Cross*, vol. 92, no. 878, pp. 437–452. DOI: 10.1017/S1816383110000366.

S. A., DSc., prof. Popov S.A., Dr. Tech. Sci., prof. Lienkov S.V., Konovaliuk M.D.

METHODOLOGICAL PRINCIPLES OF SHOOTER TRAINING AND THE USE OF SMALL ARMS IN URBAN ENVIRONMENTS

The article is devoted to the development of methodological principles for the training of shooters and the effective use of small arms in urban environments, where combat operations are characterized by confined spaces, high dynamics, and complex spatial configurations. The research is based on an analysis of contemporary combat experience gained in urban theaters of war, as well as experimental testing on specialized training grounds and in virtual and augmented reality environments. Structural, simulation, and situational modeling methods were used to replicate real urban combat conditions, including shooting in confined spaces, from non-standard positions, and in the presence of obstacles. As a result of the study, it was established that the effectiveness of small arms in urban environments is determined by their accuracy, penetration capability, ergonomics, and adaptability to rapidly changing combat situations, as confirmed by testing of compact assault rifles and submachine guns. The scientific novelty lies in the creation of a comprehensive assessment methodology that integrates the analysis of ballistic characteristics, ricochet safety, acoustic stealth, and the shooter's psychological readiness. New approaches to combat scenario modeling are proposed, taking into account the multi-level structure of urban spaces and stress factors. The obtained results make it possible to formulate substantiated recommendations for selecting optimal weapon models for units operating in urban conditions. Further research is aimed at improving virtual training systems using biometric sensors to assess the shooter's psychophysiological state under real combat conditions. The development of universal testing standards for modular weapon systems is planned to ensure their effectiveness in dynamic urban environments.

Keywords: small arms, urban environment, tactical training, urban warfare, weapon ergonomics, testing methodology, close-quarters combat.

Dr. Tech. Sci., prof. Lienkov S.V. (VIKNU)
Ph.D. Haisha O.O. (ICM CSIC, Barcelona)
Ph.D. Lenkov Y.S. (Ministry of Energy, Kyiv)
Haisha O.O. (MKU, Mykolaiv)

DOI: <http://doi.org/10.17721/2519-481X/2025/88-05>

APPLICATION OF FUZZY LOGIC METHODS TO DEVELOP A QUADCOPTER LANDING CONTROL SYSTEM

The article addresses a pressing scientific and applied problem related to the automation of the landing process of unmanned aerial vehicles, in particular quadcopters, which today occupy a leading position among the various types of drones and are widely employed in both military and civilian domains. The landing stage constitutes an obligatory phase in the operation of such aircraft, yet at the same time it is one of the most complex, since in its final stage the vehicle must ensure safe contact with a solid surface. Consequently, the development of an effective algorithm and system for automatic quadcopter landing becomes the central objective of the conducted research.

Existing landing control solutions based on ultrasonic, infrared, thermal, or radio signals require the use of additional equipment, which complicates their integration into small and medium-sized aerial platforms. In this context, the most rational approach is considered to be the use of the quadcopter's onboard camera in combination with a specially designed landing marker placed on the platform, constructed from simple geometric figures that are easily recognizable from altitude.

To achieve the stated objective, a mathematical model of quadcopter motion was created in the Matlab Simulink environment. This model takes into account the thrust of each of the four propellers, thereby enabling the reproduction of the aircraft's displacement along the coordinate axes and the simulation of landing scenarios. The automatic control system was implemented using a fuzzy controller, which operates on the basis of three input variables representing the deviations of the current coordinates from the target landing point along the x, y, and z axes. The outputs are expressed as thrust forces for each motor. A total of thirty fuzzy inference rules were constructed, ensuring adequate responsiveness to deviations from the designated trajectory and altitude.

Experimental investigations conducted in the modeling environment confirmed the effectiveness of the proposed solution. All tests demonstrated stable guidance of the quadcopter toward the designated marker and successful completion of the landing process. The average value of the static error after landing corresponds to the requirements of the technical specification and is regarded as acceptable for automated landing systems designed for platforms with limited surface area. The dynamics of the process were characterized by the absence of significant oscillations and overshoot, a smooth reduction of speed in the final phase, and reliable attainment of the designated point.

The obtained results indicate that the proposed approach possesses substantial practical value and may be effectively employed for the creation of real-world quadcopter landing control systems.

Keywords: UAV, quadcopter, automatic landing, AI control, fuzzy logic.

Introduction. At present, unmanned aerial vehicles are increasingly penetrating various sectors of modern society. In addition to their obvious military applications, they are also employed to address a wide range of civilian tasks, including those requiring a high degree of automation throughout the entire process of UAV operation. Landing constitutes one of the mandatory stages in the exploitation of aerial vehicles, while at the same time being a rather complex procedure, since at its final stage the aircraft must ensure safe and reliable contact with a solid surface [1]. It should also be emphasized that quadcopters represent one of the most extensive categories of UAVs. Consequently, the issue of providing fully automated landing of quadcopters is of considerable relevance, and it is precisely this problem that is addressed in the present study.

The objective of this work is to reduce the amount of time required from the human operator of an unmanned aerial vehicle to complete a flight mission, which can be achieved through the automation of the landing process. Moreover, provided that this process is implemented with sufficient quality, the prospect of creating fully autonomous aerial systems becomes feasible, since landing is one of the most complex operations such systems must perform.

Literature review and problem statement. A significant number of scientific and technical publications are devoted to the study of UAV motion control systems and, in particular, landing procedures. For instance, in [2], the onboard equipment of unmanned aerial vehicles intended for solving a wide spectrum of tasks is examined in detail. This includes the determination of navigational parameters such as angular velocities and accelerations, as well as the execution of navigation and control functions during flight along a predetermined trajectory. Additionally, the issues of stabilizing the angular orientation of the vehicle in flight and transmitting telemetry data on navigational parameters through the appropriate communication channel are considered.

In the majority of publications, UAVs are analyzed in the context of their application within specific sectors. Thus, [3] investigates the use of unmanned aerial vehicles in industry as a whole, as well as in particular branches, with a more detailed focus on their role in the marine sector. The text provides an extensive overview of current challenges and presents methods that may be employed for their resolution through unmanned technologies. The article also emphasizes the importance of integrating automatic control systems into UAVs and discusses both the technical aspects of drones and the interrelation between their components. An example of software used to operate unmanned aerial vehicles is also provided.

The issues of UAV control designed for specialized fields are also addressed in [4-6]. In these studies, the structure and features of control systems for UAVs designed for landing on moving platforms are proposed and described.

Although the studies mentioned above devote limited attention to the landing problem itself, they may nevertheless prove useful for the objectives of the present research. This is because, as has already been stated, during landing on a designated small-area platform, it is necessary to ensure the movement of the aircraft, which essentially corresponds to the regular flight regime. Therefore, the aforementioned works are considered valuable for addressing landing control as well.

A more comprehensive consideration of UAV landing control is found in [7]. This work describes multirotor UAVs, which, at the most basic level, include quadcopters equipped with four rotors. The article examines the possibilities of implementing an automatic takeoff and landing system for small autonomous unmanned aerial vehicles. It substantiates the use of systems based on computer vision technology, employing optical capture of marker tags. It is emphasized that, for effective localization of key points of the UAV or the landing strip in computer vision systems during automatic takeoff and landing, the use of markers is necessary. The article further provides an analysis of different marker arrangements and variations in marker tag implementations. However, it should be noted that the work is largely conceptual in nature and does not offer a ready-made solution for the development of a UAV landing control system.

An important feature of this work lies in the fact that all algorithms related to image recognition (or computer vision, as termed by the authors) are proposed to be executed on ground-based computing systems, with data from the UAV's cameras transmitted via a radio channel. Such an approach has both significant advantages and considerable drawbacks [8]. The evident advantage is the reduction of the overall weight of the aerial system due to the use of ground-based computational modules. However, a critical disadvantage is that, should communication be disrupted or lost, it would become impossible to land the vehicle in automatic mode, and in the absence of the option for manual landing, this would inevitably lead to a crash. Consequently, this study proposes not to transfer the recognition module for landing markers to ground systems but rather to simplify the corresponding algorithm by designing the marker itself in a special, maximally simplified form. This approach will form the basis for further development in the present research.

Thus, after analyzing the problem of unmanned aerial vehicle landing as well as the existing solutions, several conclusions can be drawn. First, the issue of UAV landing is of exceptional relevance due to their increasingly widespread implementation across diverse areas of modern society. Second, landing methods based on the use of ultrasonic, infrared, thermal, and radio signals require additional equipment, which makes them unsuitable for small and medium-sized vehicles. Third, from both an economic and weight-dimensional perspective, the most efficient approach is to employ the onboard camera of a quadcopter for performing landings on a prearranged platform [9]. Finally, as reference signals for such a platform, it is advisable to use an image that is clearly distinguishable from altitude and based on simple geometric primitives such as rectangles, circles, and line segments.

Consequently, there arises the necessity to develop a control system for the automatic landing of quadcopters that relies on the recognition of a specifically designed pattern indicating the designated landing site and based on AI-principles [10].

Materials and methods. During flight, the orientation of UAV propulsion units may be arbitrary with respect to the coordinate axes, taking into account the need for maneuvering and performing various turns. However, during the landing process, it is possible, without loss of generality, to impose a specific orientation of the vehicle, for example, as illustrated in Fig. 1, a. In this case, the thrust of propellers 1 and 3 determines movement along the Ox axis, while propellers 2 and 4 govern displacement along the Oy axis. It is evident that under such an arrangement, the action of the pairs of forces generated by the propellers located diagonally opposite each other does not interfere with one another: the difference in forces $F_1 - F_3$ defines movement along the Ox axis, whereas the difference $F_2 - F_4$ defines motion along the Oy axis.

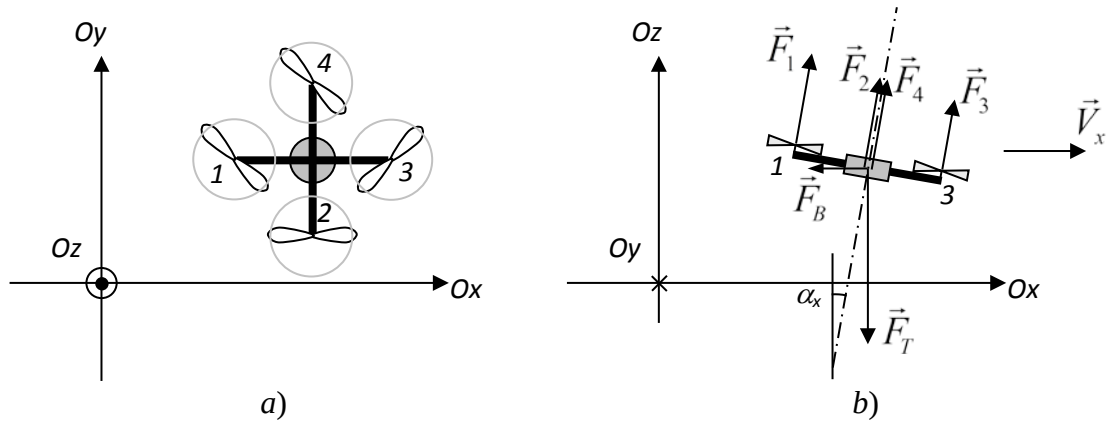


Figure 1 - Example of quadcopter orientation during landing: propellers 1–3 are responsible for displacement along the Ox axis, and propellers 2–4 are responsible for motion along the Oy axis (a top view is shown, with the Oz axis directed out of the plane of the figure): a – xOy plane, b – xOz plane

Let us now consider a case involving the difference $F_1 - F_3$, which is illustrated in the zOx plane in Fig. 1, b. Fig. 1, b shows the arrangement of forces that influence movement along the Ox axis. The complete system of equations describing the motion of the quadcopter is as follows:

$$\ddot{\alpha}_x = \frac{(F_1 - F_3)r}{I}$$

$$\ddot{\alpha}_y = \frac{(F_2 - F_4)r}{I}$$

$$\sum_{i=1}^4 F_i \cdot \sin \alpha_x - C\dot{x} = m\ddot{x}$$

$$\sum_{i=1}^4 F_i \cdot \sin \alpha_y - C \dot{y} = m \ddot{y}$$

$$\sum_{i=1}^4 F_i \cdot \cos \alpha - F_T = m \ddot{z}$$

$$\cos \alpha = \frac{1}{\sqrt{tg^2 \alpha_x + tg^2 \alpha_y + 1}}$$

Let us now examine the software implementation of the presented mathematical model describing the motion of the drone. In the idealized case of this model (in the absence of external disturbances, which sufficiently corresponds to reality under conditions without sharp wind gusts), there are four inputs representing the thrust forces of the UAV engines. These are implemented using inport blocks in the Simulink system. The outputs of the model are the three coordinates of the vehicle – x , y , and z – for which three outport blocks are used. The general view of the already implemented mathematical model is presented in Fig. 2.

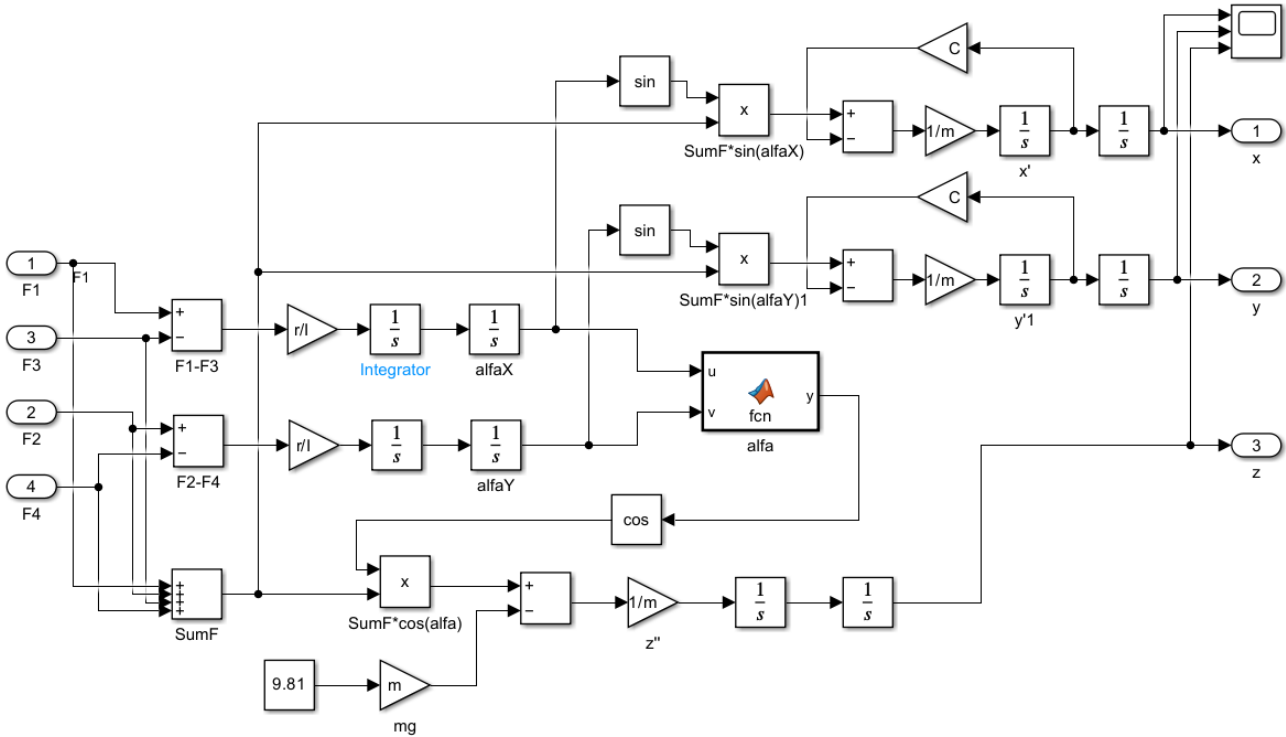


Figure 2 - Schematic representation of the mathematical model of the motion of a quadcopter-type UAV body, implemented in Matlab Simulink.

This implementation in the Simulink environment can serve as a mathematical model of the motion of a quadcopter-type unmanned aerial vehicle. This model makes it possible to test the adequacy and performance of the corresponding control system.

The automatic control system itself is implemented using a fuzzy controller [11]. In the developed control system, three input variables are defined. The first input corresponds to the difference between the current x coordinate and the coordinate x_0 of the intended landing point, denoted as Δx . For this parameter, a range from -100 to 100 meters is applied. The second input is the difference between the current y coordinate and the coordinate y_0 of the intended landing point, denoted as Δy , with the same range of -100 to 100 meters. The third input corresponds to the difference between the current z coordinate and the coordinate z_0 of the intended landing point, denoted as Δz , and for this characteristic the range from 0 to 100 meters is used.

As output variables, four thrust forces F_1 , F_2 , F_3 , and F_4 are defined, which correspond to the propellers of the quadcopter (the distribution of force numbers along the respective axes was

specified earlier and illustrated in Fig. 1). The variation range of these forces is set from 0 to 10 N. Since the modeling is performed on a small vehicle with a mass of about 2 kg, a total thrust capacity of 40 N is considered sufficient to execute rather sharp maneuvers, including rapid altitude changes.

For the input variables ΔX and ΔY , five linguistic terms are assigned: NB (Negative Big), NM (Negative Medium), Z (Zero), PM (Positive Medium), and PB (Positive Big). For the variable ΔZ , three terms are used: Z, PM, and PB. Each output linguistic variable is characterized by three terms corresponding to the values "small," "medium," and "large".

For the fuzzy control system, fuzzy inference rules were designed, amounting to a total of 30 rules, which are displayed in Fig. 3. The rules are structured in such a way that control of motion along the Ox axis and motion along the Oy axis are implemented independently, with 15 rules assigned to each axis. The number of 15 rules per axis results from the fact that the linguistic variables ΔX and ΔY are described by five terms each, while ΔZ contains three terms, leading to a total of $3 \times 5 = 15$ possible combinations for each axis.

The figure displays a software interface for defining fuzzy inference rules. At the top, a list of 14 rules is shown, each with a number and a logical statement. Below this, a rule editor is visible, showing the structure of a rule: 'If (deltaX is NB) and (deltaY is NB) and (deltaZ is Z) Then (F1 is PB) and (F2 is Z)'. Each input variable (deltaX, deltaY, deltaZ) and output variable (F1, F2) has a dropdown menu with linguistic terms: NB, NM, Z, PM, PB, and none. The 'Connection' section shows 'and' selected. At the bottom, there are buttons for 'Delete rule', 'Add rule', 'Change rule', and navigation arrows.

Figure 3 - Rule base of fuzzy productions designed for the automatic landing system of UAV.

The rules were formulated in accordance with a general logic. The greater the deviation along the x or y coordinate, the larger the difference must be between the two thrust forces responsible for movement along that axis, thereby enabling the vehicle to shift rapidly in the desired direction. At the same time, another important factor is taken into account: if the altitude is relatively high, the total value of the two forces acting along the Ox or Oy axis must not be too large, which allows for accelerated descent. Conversely, as the altitude decreases, the total thrust of each pair of propellers is reduced, ensuring a gradual and smooth descent of the quadcopter [12].

All the rules implement the previously described logic, according to which a high altitude corresponds to its rapid decrease, a large deviation along the x -axis corresponds to a significant difference in thrust between F_1 and F_3 , and a large deviation along the y -axis corresponds to a significant difference in thrust between F_2 and F_4 .

The rule base was analyzed for consistency both manually and by means of examining the fuzzy inference surfaces provided by the Matlab Fuzzy Logic Toolbox. The developed fuzzy control system was imported into the fuzzy controller, which was subsequently integrated into the overall system combining the previously constructed quadcopter body dynamics model and the control subsystem, as shown in Fig. 4. This integrated system was employed to evaluate the quality of the obtained solution, with the evaluation process described in the following subsection.

Thus, based on the individual models obtained, a comprehensive system was constructed for investigating the performance characteristics of the proposed solution, with these models incorporated as subsystems (subsystems in Simulink terminology). The results of this investigation are presented in the next subsection.

Results. For the developed system, it is essential to conduct procedures aimed at assessing the quality of its operation, and such an evaluation can be effectively carried out using the model previously implemented in Matlab Simulink. After integrating the proposed solutions into a single framework, a series of tests was performed to examine the behavior of the aerial vehicle under different input conditions.

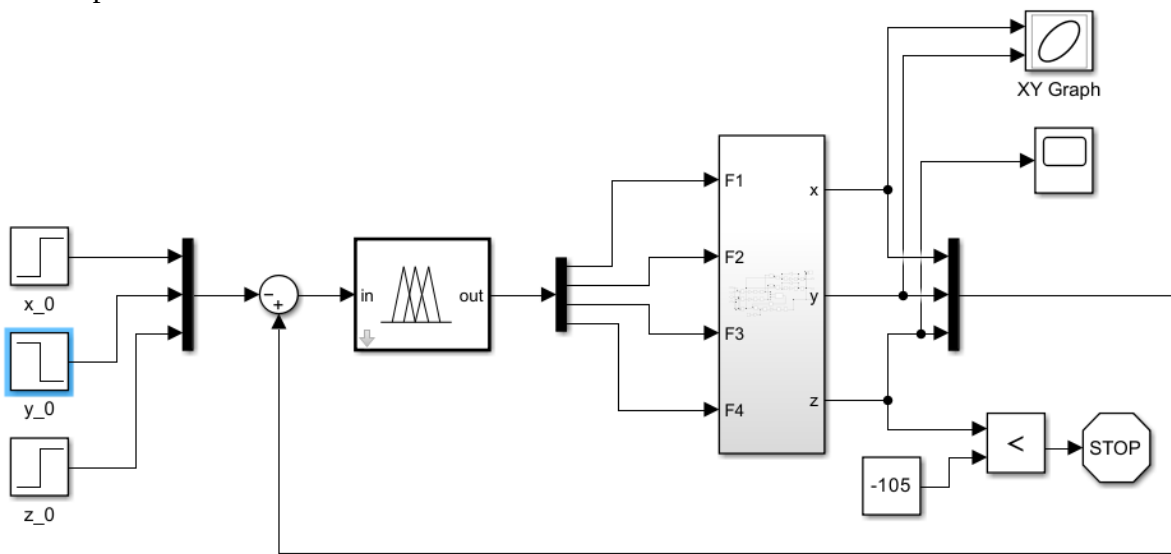


Figure 4 - System designed for testing the operation of the developed control solution.

The results of the conducted experiments revealed the following features of system behavior. The quadcopter consistently directed its motion toward the detected point of the intended landing site. The static error at the completion of the landing process did not exceed approximately 1.3 meters, which can be considered a satisfactory value for fully automated landings within a landing area of several meters in size. Overshoot was practically absent, and the landing process was predominantly aperiodic in character, ensuring stable descent dynamics. These observations are clearly illustrated in Fig. 5.

The final segment of the trajectory is shown in enlarged form in Fig. 6.

The descent in altitude corresponding to the trajectory shown in Fig. 5 is presented in Fig. 7. It is evident that the process initially occurs with a steep decline, but as the vehicle approaches the supporting surface, its motion becomes increasingly smooth and gradual.

Conclusion. Analysis of the data presented in Fig. 5, as well as in other graphs (not presented due to the limited article size), makes it possible to specify the value of the static error along the coordinates. In Fig. 5, this error amounts to approximately 1.27 meters, while the average over four experiments equals 1.2 meters. This value can be regarded as fully acceptable and corresponds to the requirements set by the technical specification for the development. On the curves shown in Fig. 3.9 (and similar), it is possible to identify distinct segments reflecting the transition from rapid motion, generated by the fuzzy control system at a considerable distance from the landing point, to medium-speed movement (in the region of $x = 80\text{--}100$), and finally to low-speed motion with precise positioning on the designated marker (approximately after $x = 100$).

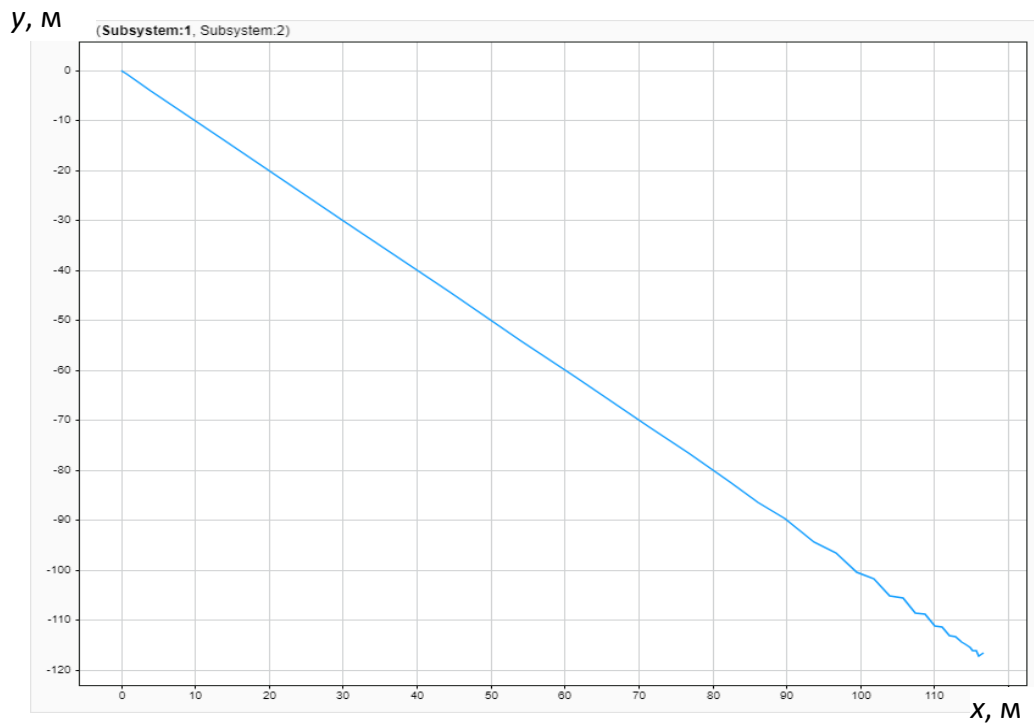


Figure 5 - Example of the quadcopter's motion from the initial point (0;0), where the landing marker was first identified, to the designated landing point, which was initially detected at coordinates (115; -115).

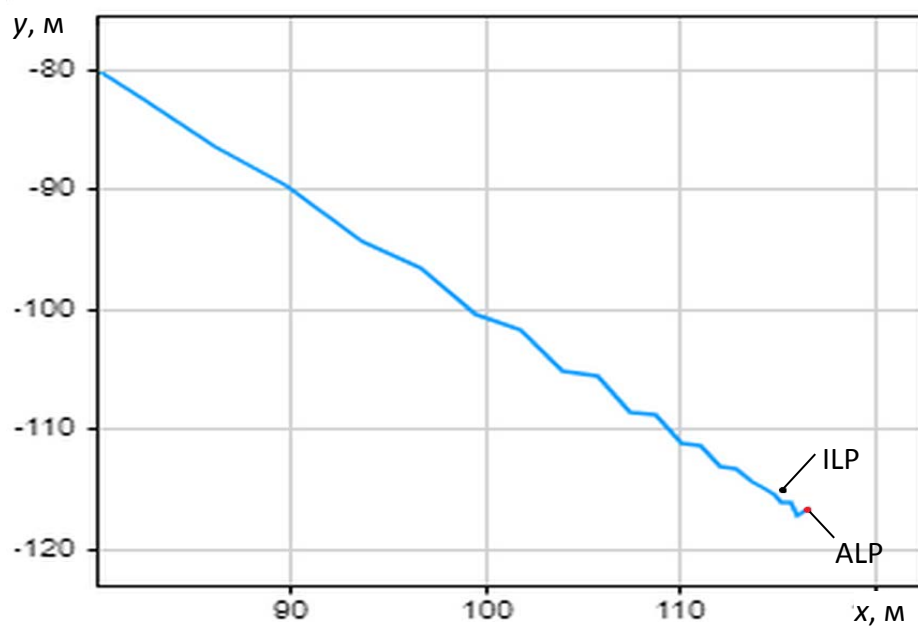


Figure 6 - Concluding part of the trajectory, displaying both the intended landing point (ILP) and the actual landing point (ALP).

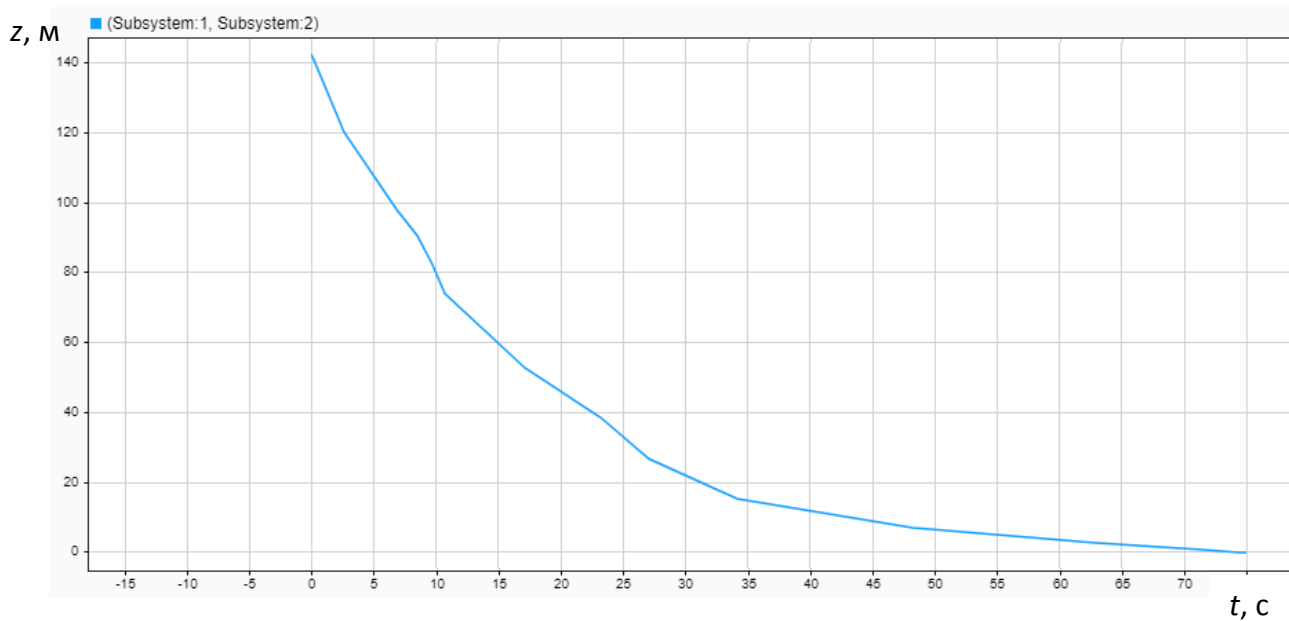


Figure 7 - Decrease in altitude over time corresponding to the motion in the xOy plane shown in Fig. 5.

Therefore, based on the analysis of the obtained results, it can be concluded that the developed solution demonstrates satisfactory performance characteristics and may be recommended for implementation in an actual aerial vehicle for the purpose of controlling automatic landing processes.

REFERENCES:

1. Long, X., Zimu, T., Weiqi, G. and Haobo, L. (2022) 'Vision-Based Autonomous Landing for the UAV: A Review', *Aerospace*, 9, p. 634.
2. Baidya, R. and Jeong, H. (2024) 'Simulation and real-life implementation of UAV autonomous landing system based on object recognition and tracking for safe landing in uncertain environments', *Frontiers in Robotics and AI*, 11, p. 1450266. doi:10.3389/frobt.2024.1450266.
3. Cho, G., Choi, J., Bae, G. and Oh, H. (2022) 'Autonomous ship deck landing of a quadrotor UAV using feed-forward image-based visual servoing', *Aerospace Science and Technology*, 130, p. 107869. doi:10.1016/j.ast.2022.107869.
4. Aikins, G., Jagtap, S. and Nguyen, K.-D. (2024) 'A robust strategy for UAV autonomous landing on a moving platform under partial observability', *Drones*, 8, p. 232. doi:10.3390/drones8060232.
5. Araar, O., Aouf, N. and Vitanov, I. (2017) 'Vision based autonomous landing of multirotor UAV on moving platform', *Journal of Intelligent and Robotic Systems*, 85, pp. 369–384. doi:10.1007/s10846-016-0399-z.
6. Kim, J., Jung, Y., Lee, D. and Shim, D.H. (2014) 'Outdoor autonomous landing on a moving platform for quadrotors using an omnidirectional camera', *2014 International Conference on Unmanned Aircraft Systems (ICUAS)*, IEEE, pp. 1243–1252.
7. Lv, M., Fan, B., Fang, J. and Wang, J. (2024) 'Autonomous Landing of Quadrotor Unmanned Aerial Vehicles Based on Multi-Level Marker and Linear Active Disturbance Reject Control', *Sensors*, 24(5), p. 1645. doi:10.3390/s24051645.
8. Chen, J., Miao, X., Jiang, H., Chen, J. and Liu, X. (2017) 'Identification of autonomous landing sign for unmanned aerial vehicle based on faster regions with convolutional neural network', *2017 Chinese Automation Congress (CAC)*, IEEE, pp. 2109–2114.
9. Ding, J., Xue, N., Xia, G.-S., Bai, X., Yang, W., Yang, M.Y. et al. (2021) 'Object detection in aerial images: a large-scale benchmark and challenges', *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 44, pp. 7778–7796. doi:10.1109/tpami.2021.3117983.

10. Wang, Y., Liu, W., Liu, J. and Sun, C. (2023) 'Cooperative USV-UAV marine search and rescue with visual navigation and reinforcement learning-based control', *ISA Transactions*, 137, pp. 222–235. doi:10.1016/j.isatra.2023.04.025.
11. Rabah, M., Haghbayan, H., Immonen, E. and Plosila, J. (2022) 'An AI-in-Loop Fuzzy-Control Technique for UAV's Stabilization and Landing', *IEEE Access*, 10, pp. 101119–101123. doi:10.1109/ACCESS.2022.3145186.
12. Bouaiss, O., Mechgoug, R. and Taleb-Ahmed, A. (2023) 'Visual soft landing of an autonomous quadrotor on a moving pad using a combined fuzzy velocity control with model predictive control', *Signal, Image and Video Processing*, 17, pp. 21–30. doi:10.1007/s11760-021-02065-0.

д.т.н., проф. **Ленков С.В.**, к.т.н., доц. **Гайша О.О.**,
к.т.н., ст. досл. **Ленков Є.С.**, **Гайша О.О.**

ЗАСТОСУВАННЯ МЕТОДІВ НЕЧІТКОЇ ЛОГІКИ ДЛЯ РОЗРОБКИ СИСТЕМИ КЕРУВАННЯ ПОСАДКОЮ КВАДРОКОПТЕРА

У статті розглянуто актуальну науково-прикладну проблему автоматизації процесу посадки безпілотних літальних апаратів, зокрема квадрокоптерів, які сьогодні посідають провідне місце серед різновидів дронів та знаходять широке застосування як у військовій, так і у цивільній сферах. Етап посадки є обов'язковою фазою експлуатації апарату, але водночас однією з найбільш складних, адже в її завершальній частині апарат має забезпечити безпечний контакт з твердою поверхнею. Саме тому розробка ефективного алгоритму та системи автоматичної посадки квадрокоптерів виступає ключовою метою проведеного дослідження.

Існуючі рішення по управлінню посадкою, засновані на ультразвукових, інфрачервоних, теплових чи радіосигналах, потребують додаткового обладнання, що ускладнює застосування їх на малих і середніх літальних апаратах. У цьому контексті найбільш раціональним підходом визнається використання штатної камери квадрокоптера та спеціально розробленого маркера на посадковій платформі, що складається з простих геометричних фігур, легко розпізнаваних з висоти.

Для досягнення мети створена математична модель руху квадрокоптера у середовищі Matlab Simulink. У моделі враховано тягу кожного з чотирьох пропелерів, що дозволяє відтворити переміщення апарату вздовж координатних осей та відпрацювати сценарій посадки. Система автоматичного керування реалізована на основі нечіткого регулятора, для якого визначено три вхідні змінні – відхилення поточних координат від цільової точки посадки за осями x , y та z . На виході формуються керуючі впливи у вигляді сил тяги для кожного двигуна. Всього побудовано 30 правил нечіткого виведення, які забезпечують адекватне реагування на відхилення від цільової траєкторії та висоти.

Проведені експериментальні дослідження у середовищі моделювання засвідчили ефективність запропонованого рішення. Усі тести показали стабільне спрямування квадрокоптера до позначеного маркера та успішне завершення процесу посадки. Середнє значення статичної похибки після посадки відповідає вимогам технічного завдання і вважається прийнятним для автоматизованих систем посадки на обмежені за площею платформи. Динаміка процесу характеризувалася відсутністю значних коливань і перевищень, плавним зниженням швидкості у фінальній фазі та впевненим досягненням позначеної точки.

Отримані результати свідчать, що запропонований підхід має достатню практичну цінність та може бути використаний для створення реальних систем керування посадкою квадрокоптерів.

Ключові слова: БПЛА, квадрокоптер, автоматична посадка, ШІ управління, нечітка логіка.

АРХІТЕКТУРА «НУЛЬОВОЇ ДОВІРИ» І ПЕРСПЕКТИВИ ЇЇ ВПРОВАДЖЕННЯ В ДЕРЖАВНИЙ СЕКТОР УКРАЇНИ

Сучасний етап розвитку інформаційних технологій супроводжується зростанням кібератак, що стають ключовим інструментом гібридної війни та впливають на безпеку державних інформаційних ресурсів. У контексті збройної агресії Росії проти України та масованих атак на критичну інфраструктуру актуальною є відмова від традиційної периметрової моделі кіберзахисту, яка в умовах розмитих мережесевих кордонів і використання хмарних сервісів втрачає ефективність. Перспективним підходом визнано архітектуру нульової довіри ZTA, що ґрунтується на принципах «ніколи не довіряй, завжди перевіряй», мінімізації привілеїв і постійному моніторингу. Метою дослідження є аналіз можливостей інтеграції архітектури нульової довіри до системи управління кібербезпекою державних мереж України з урахуванням нормативних вимог, обмежених ресурсів та підвищених ризиків у період гібридної агресії. У статті проведено огляд провідних міжнародних підходів, зокрема NIST SP 800-207, CISA Zero Trust Maturity Model та NCSC Design Principles, а також визначено бар'єри їх імплементації в українському контексті. Основні проблеми пов'язані з нормативними обмеженнями, застарілою інфраструктурою, браком кадрів і фінансовими ресурсами. Запропонована концептуальна модель передбачає поетапне впровадження ZTA на основі п'яти рівнів: управління ідентичностями, динамічний контроль доступу, мікросегментація мережі, захист даних та моніторинг із застосуванням аналітики поведінки. Модель інтегрує федеративне управління ідентичностями, багатофакторну автентифікацію, контекстну оцінку ризиків і централізовану платформу моніторингу. Очікуваним результатом є підвищення рівня кіберстійкості державних мереж без значного зниження продуктивності та забезпечення відповідності національним вимогам інформаційної безпеки.

Ключові слова: архітектура нульової довіри, zero trust, державні інформаційні системи, кібербезпека, гібридна війна, ідентифікація, мікросегментація, адаптивна автентифікація.

Вступ. Сучасний етап розвитку інформаційних технологій характеризується кардинальною трансформацією ландшафту кіберзагроз, особливо в умовах ескалації гібридної агресії. Події останніх років демонструють якісно новий рівень кіберзагроз, де кібератаки стають невід'ємною частиною воєнних дій та геополітичних протистоянь [1]. Державні мережі, які традиційно розглядаються як відносно захищені периметром системи, сьогодні стикаються з безпрецедентними за масштабом і складністю загрозами, що потребує фундаментального перегляду підходів до управління кібербезпекою.

Аналіз сучасного стану кібербезпеки державних мереж виявляє низку системних проблем в управлінні. По-перше, класична периметрова модель безпеки, що передбачає чіткий поділ на «внутрішні» та «зовнішні» загрози, втрачає ефективність в умовах розмитих кордонів мережної інфраструктури та зростаючої мобільності користувачів. По-друге, реактивний характер більшості систем управління кібербезпекою не дозволяє адекватно протидіяти складним багатоетапним атакам, характерним для державних акторів. По-третє, фрагментованість управління безпекою між різними відомствами та службами створює прогалини у загальній системі захисту [2].

Міжнародний досвід останніх років демонструє інтерес до архітектури «нульової довіри» (Zero Trust Architecture, ZTA) як до перспективного підходу до вирішення зазначених проблем. Концепція ZTA, що базується на принципі «ніколи не довіряй, завжди перевіряй», пропонує радикально інший підхід до управління кібербезпекою, де довіра не є статичним атрибутом, а динамічно оцінюється для кожного запиту на доступ до ресурсів.

Цей підхід є особливо актуальним для державних мереж, де критично важливо забезпечити безперервний контроль доступу до чутливої інформації та критичних систем.

Для державних мереж України, що функціонують в умовах повномасштабної агресії, питання інтеграції ZTA-підходів у систему управління кібербезпекою набуває особливої актуальності. Необхідність забезпечення безперервності функціонування критичних державних сервісів за умов постійного кіберпротистояння потребує не тільки технологічної модернізації, але й адаптації управлінських процесів до реалій архітектури нульової довіри.

Таким чином, актуальність даного дослідження обумовлена необхідністю наукового обґрунтування можливостей інтеграції архітектури нульової довіри до системи управління кібербезпекою державних мереж з урахуванням умов гібридної агресії та воєнного часу.

Мета роботи. Мета роботи полягає в аналізі можливостей інтеграції архітектури нульової довіри до системи управління кібербезпекою державних мереж України з урахуванням нормативних вимог, обмежених ресурсів та підвищених ризиків у період гібридної агресії.

Сучасний стан проблеми. В останнє десятиліття різні національні агенції кібербезпеки розробили власні підходи до впровадження Zero Trust Architecture у державних організаціях [3-5]. Аналіз цих підходів демонструє як загальні принципи, так і суттєві відмінності у методології та практичній реалізації.

Національний інститут стандартів та технологій США (NIST) у публікації SP 800-207 представив найбільш комплексний підхід до впровадження ZTA у державному секторі [6]. Документ визначає три фундаментальні принципи: «ніколи не довіряй, завжди перевіряй», що означає необхідність автентифікації та авторизації кожного запиту; принцип мінімальних привілеїв, згідно з яким доступ надається лише до необхідних ресурсів; та принцип «припускай порушення», що вимагає проектування системи з урахуванням можливості компрометації будь-якого елемента. SP 800-207 є фундаментальною методологією з високим рівнем деталізації і широкою застосовністю. Ключові переваги цього підходу включають комплексність архітектурних принципів, офіційну державну підтримку та універсальність для різних типів організацій. Серед обмежень слід виділити високу складність впровадження, значні вимоги до ресурсів та потенційну надмірність для невеликих державних установ з обмеженими можливостями ІТ.

Агенція з кібербезпеки і захисту інфраструктури США (CISA) розробила практико-орієнтовану модель — Zero Trust Maturity Model [7]. Ця модель визначає п'ять ключових доменів: ідентичність (Identity), пристрої (Devices), мережі (Networks), застосунки та робочі навантаження (Applications and Workloads), а також дані (Data). Для кожного домену передбачено чотири рівні зрілості: Traditional, Initial, Advanced та Optimal. Такий підхід забезпечує організаціям можливість планувати поетапний перехід до архітектури нульової довіри, виходячи з поточного рівня та цільових показників. Ключові переваги моделі включають наявність чітких індикаторів прогресу, структурованого підходу до розвитку можливостей та оптимізацію для державного сектору. Водночас модель має обмеження: орієнтація на нормативно-правову базу США, високі вимоги до ресурсів для досягнення вищих рівнів зрілості Advanced та Optimal, а також недостатнє опрацювання аспектів зручності використання.

Національний центр кібербезпеки Великобританії (NCSC) пропонує більш прагматичний підхід у своїй концепції Zero Trust Architecture Design Principles [8]. Британський підхід фокусується на п'яти ключових принципах: знання архітектури, яке передбачає глибоке розуміння існуючої інфраструктури, мережових взаємодій та потоків даних; знання користувачів, яке вимагає ефективного управління ідентичністю, обліковими записами та привілеями; знання пристроїв, яке включає контроль та керування кінцевими точками, включаючи BYOD; знання сервісів, яке охоплює захист додатків, API та хмарних сервісів; принцип недовіри до мережі, який зобов'язує реалізувати наскрізне шифрування та мікросегментацію. Даний підхід характеризується прагматичністю та гнучкістю застосування. Його переваги включають фокус на основних принципах безпеки, відносно

простоту розуміння та впровадження, а також можливість адаптації до різних організаційних контекстів. Однак цей підхід менш деталізований порівняно з американськими аналогами та потребує додаткової інтерпретації для конкретних умов впровадження.

Австралійський центр кібербезпеки (ACSC) пропонує практико-орієнтований фреймворк Essential Eight, спрямований на зниження ймовірності успішних кібератак за рахунок впровадження восьми ключових заходів захисту [9]. Даний підхід є набором мінімальних базових рекомендацій, що забезпечують захист від найбільш поширених загроз і вразливостей. Основні заходи включають: регулярне оновлення застосунків з метою усунення відомих вразливостей; своєчасне оновлення операційних систем; обов'язкова багатофакторна автентифікація для всіх критично важливих облікових записів; використання білих списків застосунків (whitelisting) для запобігання запуску несанкціонованого ПЗ; обмеження та контроль прав адміністрування; управління макросами з метою зниження ризику експлуатації вразливостей в документах; налаштування застосунків для мінімізації потенційних атак (наприклад, відключення небезпечних функцій); виконання регулярного резервного копіювання даних та перевірка відновлення. Основні переваги цього підходу полягають у простоті розуміння та реалізації, можливості поступового впровадження, оптимізації для базового захисту державних та комерційних структур. При цьому слід зазначити, що Essential Eight не є повноцінною архітектурною моделлю Zero Trust – в основному він орієнтований на мінімальний рівень захисту, недостатній для протидії цільовим АРТ-атакам і гібридним загрозам.

Специфічні проблеми впровадження ZTA в сучасних українських умовах. Впровадження ZTA у державних мережах України стикається з комплексом специфічних проблем, які потребують особливої уваги та адаптації міжнародних підходів до національних умов. Ці проблеми охоплюють нормативно-правову, технічну, економічну, організаційну та геополітичну сфери.

Для розуміння масштабу необхідних змін важливо порівняти переваги архітектури нульової довіри із традиційною периметровою моделлю, яка нині домінує в українських державних мережах. Таблиця 1 ілюструє ключові різниці між цими підходами.

Це порівняння демонструє, що перехід від периметрової моделі до ZTA вимагає фундаментального перегляду підходів до безпеки. Незважаючи на очевидні переваги архітектури нульової довіри, цей перехід пов'язаний із значними викликами в українському контексті.

Нормативно-правові виклики є однією з найбільш серйозних проблем для впровадження ZTA. Чинний Закон України «Про захист інформації в інформаційно-комунікаційних системах» [10] не містить спеціальних положень, які б регулювали принципи нульової довіри, що створює правову невизначеність при впровадженні відповідних технологій. Таким чином, необхідність гармонізації національного законодавства з вимогами Європейського союзу, включаючи GDPR [11] та директиву NIS2 [12], ускладнює процес адаптації ZTA-підходів. Відсутність національних стандартів ZTA призводить до фрагментарного та несистемного підходу до впровадження цих технологій у різних державних організаціях.

Вимоги Державної служби спеціального зв'язку та захисту інформації України, розроблені для традиційних периметрових моделей безпеки, не повністю відповідають принципам ZTA. Це створює необхідність адаптації існуючих процедур атестації та сертифікації інформаційних систем. Виникає також потенційний конфлікт між вимогами відкритості державних даних, закріпленими у Законі «Про доступ до публічної інформації» [13], та принципами обмеженого доступу, що лежать в основі архітектури нульової довіри.

Особливе занепокоєння викликають технічні обмеження, які є серйозною перешкодою для впровадження ZTA. Значна частина державних мереж побудована на застарілих технологіях, які не підтримують сучасні протоколи автентифікації та авторизації [14]. Відсутність сучасних засобів моніторингу та аналітики у більшості державних організацій унеможливорює реалізацію принципу неперервної верифікації доступу. Обмежена пропускна

спроможність каналів зв'язку, особливо у регіональних державних установах, створює додаткові труднощі застосування систем, які потребують інтенсивної мережевої взаємодії.

Кадрові проблеми посилюють технічну ситуацію [15]. Гостра нестача фахівців з кібербезпеки у державному секторі призводить до того, що багато організацій не мають достатнього експертного потенціалу для планування та реалізації проектів впровадження ZTA. Недостатній рівень знань про сучасні технології безпеки серед існуючих ІТ-фахівців потребує значних інвестицій у навчання та перепідготовку. Висока плинність кадрів у ІТ-підрозділах державних організацій, обумовлена низьким рівнем оплати праці в порівнянні з приватним сектором, створює додаткові труднощі для накопичення експертизи в галузі ZTA.

Таблиця 1

Порівняння периметрової моделі і Zero Trust Architecture

Критерій	Периметрова модель	Zero Trust Architecture
Модель довіри	Довіра – всередині периметра, недовіра – ззовні	Нікому не довіряй, завжди перевіряй
Принцип безпеки	Захист периметра	Захист кожного ресурсу
Автентифікація	Одноразова при вході до мережі	Неперервна для кожного запиту
Авторизація	Широкі права доступу всередині периметра	Мінімальні привілеї для кожного ресурсу
Сегментація	Груба сегментація по підмережам	Мікросегментація на рівні застосунків
Моніторинг	Фокус на периметрі	Моніторинг всіх взаємодій
Масштабуємість	Обмежена віддаленим доступом	Висока для розподілених середовищ
Адаптивність до загроз	Повільна реакція на внутрішні загрози	Швидке виявлення і реагування
Складність управління	Відносна проста	Висока, потребує автоматизації
Вартість впровадження	Низька для існуючих систем	Висока на початковому етапі
Сумісність з хмарними рішеннями	Обмежена	Висока
Захист від інсайдерських загроз	Слабка	Сильна

Економічні чинники є критичним обмеженням для впровадження ZTA. Обмежене фінансування IT-проектів у державному секторі, особливо в умовах воєнного часу, робить проблематичним виділення коштів на масштабні проекти модернізації безпекової інфраструктури. Висока вартість сучасних безпекових рішень, включаючи ліцензії на програмне забезпечення, обладнання та послуги інтеграції, часто перевищує бюджетні можливості державних організацій. Необхідність значних інвестицій у навчання персоналу створює додаткове фінансове навантаження на і без того обмежені IT-бюджети.

Проблеми державних закупівель додають додаткових труднощів до економічних викликів. Існуючі процедури державних закупівель, орієнтовані на стандартні товари та послуги, погано адаптовані для придбання інноваційних рішень безпеки. Відсутність спеціалізованих технічних вимог для ZTA-рішень у типовій тендерній документації призводить до закупівлі неадекватних чи неповних рішень. Обмежений вибір локальних постачальників, здатних надати комплексні ZTA-рішення, створює залежність від закордонних виробників, що є неприпустимим для державного сектору і критично важливої інфраструктури, та ускладнює процес закупівель.

Організаційні виклики включають культурні бар'єри та проблеми міжвідомчої взаємодії. Традиційний підхід до управління IT-безпекою, що базується на периметровій моделі, глибоко вкорінений в організаційній культурі державних установ. Опір змінам з боку персоналу, особливо серед керівного складу, що не має достатнього розуміння сучасних загроз кібербезпеці, уповільнює процес впровадження нових підходів. Недостатнє розуміння переваг ZTA на управлінському рівні призводить до низького пріоритету відповідних проектів у стратегічному плануванні організацій.

Складність міжвідомчої взаємодії створює додаткові перешкоди системного впровадження ZTA. Різні державні органи мають різний рівень готовності до впровадження нових технологій, що ускладнює координацію спільних проектів безпеки. Відсутність єдиного підходу до управління кібербезпекою на міжвідомчому рівні призводить до фрагментації зусиль та неефективного використання ресурсів.

Геополітичні чинники додають унікальні виклики для запровадження ZTA в умовах України. Військовий стан створює особливі вимоги до безпеки, які не завжди сумісні зі стандартними підходами до впровадження нових технологій. Необхідність забезпечення безперервності роботи критично важливих систем в умовах постійних загроз обмежує можливості масштабних змін інфраструктури. Постійні кібератаки на державну інфраструктуру вимагають фокусування ресурсів на оперативному реагуванні, що відволікає від довгострокових проектів модернізації.

Вимоги до імпортозаміщення в критично важливих системах створюють додаткові обмеження щодо вибору технологічних рішень. Необхідність використання вітчизняних чи союзних технологій може обмежувати доступ до найбільш передових ZTA-рішень, представлених на світовому ринку.

Таким чином, для успішного впровадження ZTA у державному секторі України необхідна розробка комплексного підходу, який би враховував специфіку національних умов та поетапну стратегію реалізації.

Для подолання виявлених проблем потрібна розробка комплексного підходу, який враховуватиме специфіку українських умов та забезпечуватиме поетапну стратегію впровадження ZTA. Такий підхід має включати адаптацію міжнародних методологій до національного контексту, розробку відповідної нормативної бази, створення програм підготовки кадрів, оптимізацію процедур закупівлі та забезпечення міжвідомчої координації. Особливу увагу слід приділити забезпеченню сумісності з існуючими системами та поетапному переходу від традиційних периметрових моделей до архітектури нульової довіри.

Адаптована модель ZTA для українських державних інформаційно-комунікаційних систем. Враховуючи специфічні умови та обмеження, виявлені у попередньому розділі, пропонується адаптована модель ZTA, яка враховує особливості українського державного

сектору. Ця модель базується на принципах міжнародних стандартів, але адаптована до національних умов, включаючи нормативно-правові вимоги, технічні обмеження та економічні реалії.

Запропонована архітектура будується довкола п'яти основних компонентів, кожен з яких адаптований до умов українських державних мереж:

Рівень керування ідентичністю та доступом є фундаментом архітектури. Цей рівень забезпечує централізоване керування користувачами, їх атрибутами та правами доступу. Для державних організацій пропонується інтеграція з існуючими системами управління персоналом та адаптація до вимог українського законодавства щодо захисту персональних даних. Компонент включає підсистеми багатофакторної автентифікації, керування життєвим циклом користувачів та федеративного доступу між різними державними організаціями.

Рівень контролю доступу до ресурсів забезпечує динамічне ухвалення рішень щодо надання доступу на основі комплексного аналізу контекстної інформації. Цей рівень включає чотири ключові компоненти:

- механізм поведінкової аналітики – аналізує патерни поведінки користувачів та виявляє аномалії у їхніх діях;
- аналізатор пристроїв та мережного контексту – оцінює характеристики пристроїв, розташування підключення та параметри мережного середовища;
- система класифікації даних – забезпечує відповідність різним рівням таємності інформації та інтеграцію із системами класифікації державних даних;
- підсистема геополітичного контексту – унікальний компонент, який аналізує поточну геополітичну обстановку, рівень кіберзагроз, статус інформаційних конфліктів та інтегрується з національними системами моніторингу загроз для коригування рівнів довіри у режимі реального часу.

Рівень мікросегментації мережі забезпечує ізоляцію ресурсів та контроль трафіку на гранулярному рівні. Компонент включає програмно-визначені периметри, динамічні правила фільтрації трафіку та системи виявлення аномалій. Для державних мереж передбачено сумісність із існуючими системами класифікації трафіку та вимогами до аудиту мережевих підключень.

Рівень захисту даних забезпечує наскрізне шифрування, класифікацію та контроль доступу до даних незалежно від їхнього розташування. Компонент включає системи запобігання витоку даних DLP, управління правами на цифрову інформацію та забезпечення цілісності даних. Для українських державних організацій передбачено інтеграцію з національними системами електронного документообігу та відповідність вимогам законодавства про захист державної таємниці.

Рівень моніторингу та аналітики забезпечує безперервний моніторинг безпеки, аналіз поведінки користувачів та автоматичне реагування на загрози. Компонент включає системи збирання та кореляції подій безпеки, машинного навчання для виявлення аномалій та автоматизованого реагування на інциденти. Для державного сектору передбачено інтеграцію з національними системами моніторингу кібербезпеки та відповідність вимогам до звітності про інциденти.

Адаптація міжнародних підходів до українських умов ґрунтується на кількох ключових принципах:

1. Принцип поетапності передбачає поступовий перехід від існуючих периметрових моделей до архітектури нульової довіри без порушення безперервності роботи критично важливих систем.
2. Принцип сумісності забезпечує інтеграцію з існуючими системами та технологіями, мінімізуючи необхідність повної заміни інфраструктури.
3. Принцип відповідності вимагає адаптації до національних нормативно-правових вимог та стандартів безпеки.

4. Принцип економічної ефективності передбачає оптимізацію витрат за впровадження та експлуатацію системи з урахуванням бюджетних обмежень державного сектора.
5. Принцип масштабованості забезпечує можливість розширення системи на різні рівні державного управління від місцевих адміністрацій до центральних органів влади.
6. Принцип стійкості до загроз враховує специфіку геополітичної ситуації та вимоги щодо забезпечення безпеки в умовах підвищених кіберзагроз.

Технічна реалізація запропонованої архітектури включає декілька ключових компонентів:

- *Центральний контролер політик* забезпечує централізоване управління правилами доступу та безпековими політиками. Цей компонент інтегрується з існуючими системами управління та забезпечує однакове застосування політик безпеки у всіх підключених організаціях.
- *Точки застосування політик* розгортаються на різних рівнях мережної інфраструктури та забезпечують контроль доступу до ресурсів відповідно до рішень центрального контролера. Ці компоненти можуть бути реалізовані як програмні агенти, інтегровані в існуючі системи або як спеціалізовані апаратні пристрої.
- *Система керування ідентичністю* забезпечує автентифікацію користувачів та керування їх атрибутами. Для державного сектора передбачена інтеграція із системами електронної ідентифікації громадян та державних службовців.
- *Система контекстної аналітики* забезпечує аналіз ризиків та прийняття рішень на основі поведінкових патернів, характеристик пристроїв та мережевого контексту.

Проводячи порівняльний аналіз запропонованої адаптованої моделі ZTA з розглянутими вище аналогами, слід підкреслити її фундаментальні відмінності.

Ключова відмінність полягає у додаванні компонента геополітичного контексту, який враховує підвищені кіберзагрози та вимоги до забезпечення національної безпеки. На відміну від базової моделі NIST, архітектура, що пропонується, включає спеціалізовані механізми для роботи з класифікованою інформацією різних рівнів секретності та інтеграцію з національними системами криптографічного захисту. Крім того, в моделі додаються специфічні компоненти для державного сектора, такі як федеративне управління ідентичністю між різними державними організаціями, інтеграція із системами електронного документообігу та відповідність вимогам національного законодавства щодо захисту персональних даних. Модель також передбачає поетапний перехід із урахуванням бюджетних обмежень державного сектора.

Етапи впровадження адаптованої моделі. Перехід від традиційної периметрової моделі до архітектури нульової довіри потребує структурованого підходу, який мінімізує ризики порушення роботи існуючих систем та забезпечує поетапне підвищення рівня безпеки. Запропонована модель впровадження складається з п'яти незалежних етапів, кожен із яких представляє самостійну цінність і може бути реалізований незалежно від інших.

Для забезпечення ефективного управління процесом впровадження запропонованої моделі визначені критерії успішності кожного етапу та оцінки їх кількісних характеристик, при цьому обґрунтування і уточнення конкретних виразів останніх є результатами дослідження авторів, які зараз готуються до друку, тому не приводяться детально в цій роботі.

Етап 1: Інвентаризація та аналіз існуючої інфраструктури. Перший етап фокусується на детальному аналізі поточного стану інформаційних систем та мережевої інфраструктури державної організації. Мета етапу полягає у створенні повної карти цифрових активів,

розумінні потоків даних та ідентифікації критично важливих ресурсів, що потребують пріоритетного захисту.

Інвентаризація включає автоматизоване сканування мережної інфраструктури з метою виявлення всіх підключених пристроїв, серверів, робочих станцій і мережного устаткування. Аналіз програмних активів охоплює всі встановлені застосунки, операційні системи, бази даних та мережеві послуги. Особлива увага приділяється виявленню застарілих систем, які можуть становити загрозу безпеці.

Картування потоків даних включає аналіз всіх інформаційних обмінів між системами, виявлення критично важливих даних та шляхів їх обробки. Проводиться класифікація даних щодо рівня конфіденційності відповідно до вимог українського законодавства. Аналізуються існуючі механізми захисту даних та виявляються прогалини у їх покритті.

Оцінка ризиків безпеки включає аналіз вразливостей у існуючих системах, моделювання потенційних загроз та оцінку можливої шкоди від їх реалізації. Проводиться аналіз відповідності існуючих заходів безпеки вимогам національних стандартів та найкращих міжнародних практик.

Результатом першого етапу є створення детальної карти цифрової інфраструктури, реєстру критично важливих активів, класифікації даних за рівнями конфіденційності та пріоритизованого списку загроз безпеці. Ця інформація є основою для планування наступних етапів впровадження ЗТА.

Успішність першого етапу оцінюється за повнотою та якістю проведеної інвентаризації та аналізу.

Критерій повноти інвентаризації передбачає виявлення 93–97% всіх цифрових активів організації, включаючи сервери, робочі станції, мережне устаткування й програмні системи. Якість інвентаризації оцінюється за точністю класифікації активів, коректністю визначення їх критичності та за повнотою опису залежностей між системами.

Критерій якості аналізу потоків даних передбачає картування всіх критично важливих інформаційних обмінів та визначення шляхів обробки конфіденційної інформації. Успішність оцінюється за відповідністю класифікації даних вимогам національного законодавства та повноті виявлення потенційних точок витоку інформації.

Критерій ефективності оцінки ризиків включає виявлення всіх критичних вразливостей у існуючих системах та пріоритизацію загроз відповідно до їх потенційного впливу на організацію. Успішність етапу підтверджується створенням детального плану усунення виявлених вразливостей та чітким розумінням поточного рівня ризику.

Етап 2: Впровадження централізованого управління ідентичністю. Другий етап фокусується на створенні єдиної системи управління ідентичності та доступом, яка стане фундаментом для всіх наступних компонентів архітектури нульової довіри. Мета етапу полягає в централізації управління користувачами, стандартизації процедур автентифікації та створенні основи для застосування принципу мінімальних привілеїв.

Розгортання системи управління ідентичністю починається із створення центрального репозиторію користувачів, який інтегрується з існуючими системами управління персоналом. Передбачається інтеграція із національними системами електронної ідентифікації для забезпечення відповідності вимогам законодавства.

Впровадження багатофакторної автентифікації включає розгортання додаткових факторів автентифікації, крім традиційних паролів. Система підтримує різні методи автентифікації, включаючи SMS-коди, мобільні застосунки, апаратні токени та біометричні дані. Для державного сектора передбачена інтеграція із системами електронного підпису та відповідність вимогам до криптографічного захисту.

Створення системи управління правами доступу включає визначення ролей та дозволів відповідно до організаційної структури та функціональних обов'язків користувачів. Система забезпечує автоматичне призначення прав доступу на основі посадових інструкцій та автоматичне відкликання доступу при зміні статусу користувача. Передбачається інтеграція

із системами управління життєвим циклом користувачів для автоматизації процесів надання та відкликання доступу.

Результатом другого етапу є створення централізованої системи управління ідентичністю, впровадження багатофакторної автентифікації для всіх користувачів, створення структурованої системи управління правами доступу та забезпечення єдиного входу до корпоративних застосунків. Цей етап значно підвищує рівень безпеки організації та створює основу для наступних етапів запровадження ZTA.

Успішність другого етапу оцінюється за ефективністю впровадження централізованого управління ідентичністю та якістю інтеграції з існуючими системами.

Критерій охоплення користувачів передбачає включення до системи управління ідентичністю не менше 100% активних користувачів організації з коректним визначенням їх ролей та дозволів.

Критерій ефективності багатофакторної автентифікації передбачає впровадження додаткових факторів автентифікації для всіх користувачів з привілейованим доступом і для 78–85% звичайних користувачів. Успішність оцінюється за зниженням кількості інцидентів, пов'язаних з компрометацією облікових записів, та відповідністю вимогам національних стандартів безпеки.

Критерій якості управління правами доступу включає автоматизацію процесів надання та відкликання доступу для 90–95% користувачів організації. Успішність підтверджується відповідністю принципу мінімальних привілеїв та відсутністю надлишкових прав доступу у користувачів.

Етап 3: Реалізація динамічного контролю доступу. Третій етап фокусується на створенні системи динамічного контролю доступу, яка приймає рішення про надання доступу на основі аналізу багатьох факторів ризику. Мета етапу полягає у переході від статичних правил доступу до динамічної оцінки ризику та адаптивного контролю доступу.

Розгортання системи оцінки ризиків включає створення механізмів аналізу контекстної інформації кожного запиту доступу. Система аналізує поведінкові патерни користувачів, характеристики пристроїв, розташування, час доступу та інші контекстні фактори. Для державного сектора передбачено інтеграцію із системами класифікації інформації та облік вимог до різних рівнів секретності.

Використання адаптивної автентифікації забезпечує застосування додаткових заходів автентифікації залежно від рівня ризику. Система може вимагати додаткову автентифікацію для доступу до критично важливих ресурсів у випадку виявлення аномальної поведінки або запиту на доступ з невідомих пристроїв. Передбачається інтеграція із системами аналізу поведінки користувачів для автоматичного виявлення аномалій.

Створення системи контекстного аналізу включає впровадження механізмів збирання та аналізу інформації про контекст доступу. Система аналізує мережеве оточення, характеристики пристроїв, геолокацію та часові патерни доступу. Для державних організацій передбачена інтеграція із системами моніторингу безпеки та відповідність вимогам до аудиту доступу.

Впровадження динамічних політик доступу забезпечує автоматичну зміну правил доступу залежно від зміни безпекових умов. Система може автоматично обмежувати доступ при виявленні загроз, змінювати вимоги до автентифікації залежно від рівня ризику та застосовувати додаткові заходи захисту для критично важливих ресурсів.

Результатом третього етапу є створення системи динамічного контролю доступу, впровадження адаптивної автентифікації, створення механізмів контекстного аналізу та застосування динамічних безпекових політик. Цей етап значно підвищує здатність організації до виявлення та запобігання загрозам безпеки. Саме на цьому етапі активується підсистема геополітичного контексту рівня контролю доступу до ресурсів.

Успішність третього етапу оцінюється за ефективністю системи динамічного контролю доступу та якістю оцінки ризиків.

Критерій точності оцінки ризиків передбачає досягнення не менше 90% точності у визначенні рівня ризику для запитів доступу з мінімальною кількістю помилкових спрацьовувань.

Критерій ефективності адаптивної автентифікації включає автоматичне застосування додаткових заходів автентифікації для 95–97% високоризикових запитів доступу. Успішність оцінюється за зниженням кількості успішних атак на системи організації та відповідністю часу відгуку вимогам користувачів.

Критерій якості контекстного аналізу передбачає облік не менше п'яти різних факторів ризику при прийнятті рішень про доступ, включаючи поведінкові патерни, характеристики пристроїв та мережевий контекст. Успішність підтверджується підвищенням здатності системи до виявлення аномальної поведінки та запобіганням несанкціонованому доступу.

Етап 4: Впровадження мікросегментації мережі. Четвертий етап фокусується на створенні мікросегментованої мережевої архітектури, яка забезпечує ізоляцію ресурсів та контроль трафіку на гранулярному рівні. Мета етапу полягає у заміні традиційної моделі «довіри всередині периметра» на модель «нульової довіри до мережі».

Впровадження програмно-визначуваних периметрів включає створення безпечних каналів зв'язку між авторизованими користувачами та ресурсами. Система створює індивідуальні зашифровані тунелі для кожного користувача, забезпечуючи ізоляцію трафіку та приховування ресурсів від неавторизованих користувачів. Для державного сектору передбачено інтеграцію з національними системами криптографічного захисту та відповідність вимогам до захисту державної таємниці.

Створення системи мікросегментації передбачає логічний поділ мережної інфраструктури на невеликі сегменти з контрольованою взаємодією між ними. Кожен сегмент містить мінімальний набір ресурсів, необхідні виконання конкретних наперед визначених функцій. Система забезпечує детальний контроль трафіку між сегментами та автоматичне застосування політик безпеки.

Впровадження системи інспекції трафіку забезпечує глибокий аналіз всіх мережевих з'єднань та виявлення потенційних загроз. Система аналізує вміст трафіку, виявляє аномальні патерни та автоматично блокує підозрілі з'єднання. Для державних мереж передбачено інтеграцію з національними системами моніторингу кібербезпеки та відповідність вимогам до звітності про мережеві інциденти.

Розгортання системи автоматичного реагування включає створення механізмів швидкого реагування на виявлені загрози. Система може автоматично ізолювати скомпрометовані сегменти, блокувати підозрілий трафік та застосовувати додаткові заходи захисту. Передбачається інтеграція із системами управління інцидентами та відповідність вимогам до процедур реагування на кіберінциденти.

Результатом четвертого етапу є створення мікросегментованої мережевої архітектури, впровадження програмно-визначуваних периметрів, створення системи глибокої інспекції трафіку та автоматичного реагування на загрози. Цей етап значно підвищує здатність організації до локалізації загроз та запобігання їх поширенню.

Успішність четвертого етапу оцінюється за ефективністю мікросегментації мережі та якістю контролю трафіку.

Критерій повноти сегментації передбачає створення ізольованих сегментів для всіх критично важливих ресурсів з контрольованою взаємодією між ними.

Критерій ефективності контролю трафіку включає інспекцію 100% мережевого трафіку з автоматичним виявленням та блокуванням підозрілих з'єднань. Успішність оцінюється за зниженням часу виявлення загроз і підвищенням ефективності їх локалізації.

Критерій якості ізоляції загроз передбачає автоматичне обмеження поширення загроз у межах одного сегмента мережі. Успішність підтверджується відсутністю випадків поширення шкідливого коду за межі скомпрометованого сегмента.

Етап 5: Впровадження комплексного моніторингу та аналітики. П'ятий етап фокусується на створенні комплексної системи моніторингу безпеки та аналітики, яка

забезпечує безперервний контроль стану безпеки та автоматичне виявлення загроз. Мета етапу полягає у створенні системи ситуаційної поінформованості про стан кібербезпеки та забезпечення швидкого реагування на інциденти.

Впровадження системи збору та кореляції подій включає створення централізованої платформи для агрегації безпекових даних з усіх компонентів інфраструктури. Система збирає логи безпеки, події автентифікації, мережеву телеметрію та іншу інформацію щодо стану безпеки. Для державного сектору передбачено інтеграцію з національними системами моніторингу та відповідність вимогам до зберігання та обробки даних про безпеку.

Створення системи поведінкової аналітики передбачає використання алгоритмів машинного навчання для аналізу поведінки користувачів та виявлення аномалій. Система створює базові профілі нормальної поведінки для кожного користувача та автоматично виявляє відхилення, які можуть вказувати на компрометацію облікових записів або інсайдерські загрози. Передбачається адаптація алгоритмів до специфіки державного сектору та інтеграція із системами управління персоналом.

Впровадження системи аналізу загроз включає створення механізмів автоматичного виявлення та класифікації кіберзагроз. Система аналізує індикатори компрометації, зіставляє їх із базами даних загроз і автоматично визначає рівень ризику. Для державного сектору передбачено інтеграцію з національними системами обміну інформацією про загрози та відповідність вимогам до класифікації інцидентів.

Створення системи автоматизованого реагування включає розробку сценаріїв автоматичного реагування на різні типи кіберінцидентів. Система може автоматично блокувати скомпрометовані облікові записи, ізолювати заражені пристрої, застосовувати додаткові заходи автентифікації та повідомляти служби безпеки про критичні інциденти. Передбачається інтеграція із системами управління інцидентами та відповідність процедурам реагування на кіберінциденти.

Результатом п'ятого етапу є створення комплексної системи моніторингу безпеки, запровадження поведінкової аналітики, створення системи аналізу загроз та автоматизованого реагування. Цей етап завершує створення повноцінної архітектури нульової довіри та забезпечує організацію сучасними засобами захисту від кіберзагроз.

Успішність п'ятого етапу оцінюється за ефективністю системи моніторингу та якістю аналітики безпеки.

Критерій повноти моніторингу передбачає збирання та аналіз даних про безпеку від усіх компонентів інфраструктури зі створенням єдиної картини стану безпеки.

Критерій ефективності виявлення загроз включає автоматичне виявлення щонайменше 95% відомих типів загроз із мінімальною кількістю помилкових спрацьовувань. Успішність оцінюється за зниженням часу виявлення інцидентів і підвищенням точності їх класифікації.

Критерій якості автоматизованого реагування передбачає автоматичне застосування відповідних заходів реагування для 80–85% виявлених інцидентів. Успішність підтверджується зниженням часу реагування на загрози та підвищенням ефективності їх нейтралізації.

Загальний критерій успішності впровадження запропонованої моделі передбачає досягнення вимірюваного підвищення рівня безпеки організації, відповідності вимогам національних стандартів безпеки та забезпечення безперервності роботи критично важливих систем протягом усього процесу впровадження.

Оцінка ризиків впровадження. Впровадження запропонованої моделі пов'язане з певними ризиками, які умовно можуть бути класифіковані на декілька груп, а саме: технічні, безпекові, організаційні та економічні. Тут ми пропонуємо спочатку розглянути технічні та безпекові ризики, як такі, які мають найбільше значення з нашої точки зору при імплементації архітектури безпеки.

До технічних ризиків належать:

- *Ризик сумісності* (високий рівень). Впровадження ZTA може призвести до конфліктів із існуючими системами та технологіями. Для мінімізації ризику пропонується

поетапний підхід із попереднім тестуванням сумісності та розробкою перехідних рішень.

- *Ризик продуктивності* (середній рівень). Додаткові рівні перевірки та шифрування можуть знизити продуктивність системи. Рекомендується використання апаратного прискорення криптографічних операцій та оптимізація алгоритмів прийняття рішень.
- *Ризик складності управління* (високий рівень). Збільшення кількості політик безпеки може призвести до помилок конфігурації. Пропонується розробка автоматизованих інструментів управління та навчання персоналу.

До безпекових ризиків належать:

- *Ризик виникнення нових векторів атак* (середній рівень). Складність системи може створити нові вразливості. Рекомендується регулярний аудит безпеки та тестування на проникнення.
- *Ризик відмови в обслуговуванні* (високий рівень). Централізовані компоненти можуть бути точкою відмови. Пропонується створення резервованих систем та планів аварійного відновлення.
- *Ризик компрометації центральних компонентів* (високий рівень). Атака на центральні компоненти може спричинити компрометацію всієї системи. Потрібні додаткові заходи захисту критично важливих компонентів.

Для мінімізації виявлених ризиків пропонується комплексний підхід, що включає технічні рішення (дублювання критично важливих компонентів, автоматизація процесів, використання відкритих стандартів), організаційні заходи (навчання персоналу, створення центру компетенцій, розробка процедур управління змінами) та економічні інструменти (поетапне фінансування, залучення міжнародних грантів).

Реалізація запропонованих заходів дозволить знизити загальний рівень ризиків впровадження з високого до прийнятного рівня та забезпечить успішний перехід до архітектури нульової довіри в українських державних мережах.

Висновки. Проведене дослідження проблем впровадження архітектури нульової довіри у державному секторі України та розроблені пропозиції щодо їх вирішення дозволяють зробити наступні висновки.

Аналіз сучасних кіберзагроз та вразливостей традиційних периметрових моделей безпеки демонструє критичну необхідність переходу українських державних організацій до архітектури нульової довіри. Традиційна модель «довіри всередині периметра» демонструє свою неефективність в умовах сучасних кібератак, особливо з огляду на специфіку геополітичної ситуації в Україні.

Пряме застосування міжнародних стандартів та методологій ZTA в українських умовах неможливе без їх суттєвої адаптації до національних особливостей. Розроблена адаптована модель враховує специфіку українського контексту та включає унікальні компоненти, які не представлені у базових міжнародних стандартах.

Ключовим нововведенням є включення компонента геополітичного контексту, що аналізує поточну геополітичну ситуацію та коригує рівні довіри залежно від зовнішніх загроз. Модель також передбачає інтеграцію з національними системами криптографічного захисту, електронного документообігу та класифікації державної інформації.

Перехід до архітектури нульової довіри забезпечить державним структурам значні переваги: підвищення адаптивності до нових видів атак, покращення можливостей

моніторингу та реагування на інциденти, посилення захисту від інсайдерських загроз, а також підвищення загального рівня кібербезпеки критично важливої інфраструктури.

ЛІТЕРАТУРА:

1. Zhou Z., Duan D., Xu H. Zero-Trust Zero-Communication Defence against Hybrid Cyberattacks in Distributed Energy Resources Using Mean Field Reinforcement Learning. *Energies*. 2024. 17(20). 5057.
2. Nisha T N, Dhanya Pramod, Ravi Singh. Zero trust security model: Defining new boundaries to organizational network. *Proceedings of the 2023 15th International Conference on Contemporary Computing (IC3-2023)*. New York, NY, USA, 2023. P. 603–609.
3. Executive Order No. 14028, 3 C.F.R. 14028 (2021). <https://public-inspection.federalregister.gov/2021-10460.pdf> (дата звернення: 20.06.2025).
4. The Department of Homeland Security. Zero Trust Implementation Strategy. URL: https://www.dhs.gov/sites/default/files/2024-02/24_0129_cio_zero_trust_implementation_strategy_october.pdf (дата звернення: 20.06.2025).
5. Phiayura P., Teerakanok S. A Comprehensive Framework for Migrating to Zero Trust Architecture. *IEEE Access*. 2023. 11. C. 19487–19511.
6. NIST SP 800-207. Zero Trust Architecture. National Institute of Standards and Technology, 2020. 59 p.
7. Cybersecurity and Infrastructure Security Agency. Zero Trust Maturity Model, Version 2.0. URL: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf (дата звернення: 20.06.2025).
8. The National Cyber Security Centre. Zero trust architecture design principles. URL: <https://www.ncsc.gov.uk/collection/zero-trust-architecture> (дата звернення: 20.06.2025).
9. Australian Cyber Security Centre. Essential Eight. URL: <https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eight> (дата звернення: 20.06.2025).
10. Про захист інформації в інформаційно-комунікаційних системах (назва Закону із змінами, внесеними згідно із Законом № 1089-IX від 16.12.2020): Закон України. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.
11. Регламент (ЄС) 2016/679 Європейського парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС. URL: <https://www.kmu.gov.ua/storage/app/sites/1/55-GOEEI/reglament-es-2016679.pdf> (дата звернення: 20.06.2025).
12. Директива Європейського Парламенту і Ради (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого спільного рівня кібербезпеки на всій території Союзу, внесення змін до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972 та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2). URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22 (дата звернення: 20.06.2025).
13. Про доступ до публічної інформації: Закон України. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314.
14. Худолій А. Кібербезпека: сучасні виклики перед Україною. *Acta De Historia & Politica: Saeculum XXI*. 2019. Вип. 1. С. 138–146.
15. Євсюкова О.В. Особливості підготовки фахівців у сфері кібербезпеки: сучасні виклики та перспективи. *Державне управління: удосконалення та розвиток*. 2021. Вип. 2. URL: <https://doi.org/10.32702/2307-2156-2021.2.2> (дата звернення: 20.06.2025).

REFERENCES:

1. Zhou, Z., Duan, D., and Xu H. (2024). “Zero-Trust Zero-Communication Defence against Hybrid Cyberattacks in Distributed Energy Resources Using Mean Field Reinforcement Learning”, *Energies*, 17(20), 5057. Available at: <https://doi.org/10.3390/en17205057>
2. Nisha T N, DhanyaPramod, and Ravi Singh. (2023). “Zero trust security model: Defining new boundaries to organizational network”, *Proceedings of the 2023 Fifteenth International Conference on Contemporary Computing (IC3-2023)*. New York, NY, USA, pp. 603–609.
3. Executive Order No. 14028, 3 C.F.R. 14028 (2021). Available at: <https://public-inspection.federalregister.gov/2021-10460.pdf> (Accessed: 20.06.2025).
4. The Department of Homeland Security. *Zero Trust Implementation Strategy*. Available at: https://www.dhs.gov/sites/default/files/2024-02/24_0129_cio_zero_trust_implementation_strategy_october.pdf (Accessed: 20.06.2025).

5. Phiayura, P., and Teerakanok, S. (2023). "A Comprehensive Framework for Migrating to Zero Trust Architecture", *IEEE Access*, 11, pp. 19487–19511. Available at: <https://doi.org/10.1109/ACCESS.2023.3248622>.
6. National Institute of Standards and Technology (NIST). (2020). *Zero Trust Architecture* (NIST Special Publication 800-207).
7. Cybersecurity and Infrastructure Security Agency. *Zero Trust Maturity Model, Version 2.0*. Available at: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf (Accessed: 20.06.2025).
8. The National Cyber Security Centre. *Zero trust architecture design principles*. Available at: <https://www.ncsc.gov.uk/collection/zero-trust-architecture> (Accessed: 20.06.2025).
9. Australian Cyber Security Centre. *Essential Eight*. Available at: <https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eight> (Accessed: 20.06.2025).
10. The Law of Ukraine "On information protection in information and communication systems". 1994. *Vidomosti Verchvnoy Rady Ukrainy*. 31. p. 286.
11. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (2016) Official Journal L 119, 1-88. <http://data.europa.eu/eli/reg/2016/679/oj>
12. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
13. The Law of Ukraine "On Access to Public Information". 2011. *Vidomosti Verchvnoy Rady Ukrainy*. 32. p. 314.
14. Khudoliy, A. (2019). "Kiberbezbeza: suchasni vyklyky pered Ukrainoyu" [Cybersecurity: modern challenges of Ukraine] *Acta De Historia & Politica: Saeculum XXI*, 1, pp. 138–146. Available at: <https://doi.org/10.26693/ahpsxxi2019.01.138>
15. Evsyukova, O. (2021). "Osoblyvosti pidgotovky fakhivtsiv u sferi kiberbezpeky: suchasni vyklyky s perspektyvy" [Features of training of specialists in the field of cyber security: current challenges and prospects]. *Derzhavne Upravlinnya: Udoskonalennya ta Rozvytok*. 2. Available at: <https://doi.org/10.32702/2307-2156-2021.2.2>

DSc, Prof. Bobok I.I., DSc, Prof. Kobozieva A.A.

ZERO TRUST ARCHITECTURE AND PROSPECTS FOR ITS IMPLEMENTATION IN THE GOVERNMENT SECTOR OF UKRAINE

The escalation of cyberattacks as a key component of hybrid warfare poses significant challenges to the security of state information systems. In the context of ongoing military aggression against Ukraine and large-scale attacks targeting critical infrastructure, the traditional perimeter-based security model has proven insufficient under conditions of blurred network boundaries and widespread adoption of cloud technologies and remote access. A promising alternative is the Zero Trust Architecture (ZTA), built on the principles of "never trust, always verify," least privilege access, and continuous monitoring. The aim of this study is to substantiate an adapted ZTA implementation model for Ukrainian government networks, considering national regulatory requirements, limited financial and human resources, and heightened risks during hybrid aggression. The paper provides an overview of leading international frameworks, including NIST SP 800-207, CISA Zero Trust Maturity Model, and NCSC Design Principles, and identifies key barriers to their application in Ukraine. These barriers include outdated infrastructure, regulatory inconsistencies, insufficient personnel expertise, and restricted budgets. The proposed conceptual model incorporates a phased implementation strategy across five layers: identity and access management, dynamic access control, network microsegmentation, data protection, and continuous monitoring with behavioral analytics. The model also integrates federated identity management, multi-factor authentication, contextual risk-based access control, and centralized monitoring via SIEM and SOAR platforms. The expected result is an increased level of cyber resilience in government networks without a significant reduction in usability, ensuring compliance with national cybersecurity standards and readiness for hybrid threats.

Keywords: zero trust, government information systems, cybersecurity, hybrid warfare, identity, microsegmentation, adaptive authentication.

МЕТОД ТА АЛГОРИТМИ ВИЯВЛЕННЯ КІБЕРАТАК В МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ НА ОСНОВІ АНАЛІЗУ ЕНЕРГОСПОЖИВАННЯ

«Розумний дім» – це система для керування основними процесами життєзабезпечення як невеликих систем (комерційні, офісні приміщення, квартири, котеджі), так і великих автоматизованих комерційних та промислових комплексів. Важливим завданням, яке має вирішувати концепція сучасного «Розумного дому», є запобігання поширенню шкідливого програмного забезпечення в інфраструктурі Інтернету речей (IoT). Незважаючи на велику кількість розроблених методів виявлення та запобігання кібератакам, IoT-пристрої все ще надзвичайно вразливі та зазнають широкого спектру кібератак, що має як фінансові, так і репутаційні наслідки. Тому існує потреба в розробленні нових підходів для виявлення шкідливого програмного забезпечення в інфраструктурі IoT. Одним з можливих підходів для виявлення аномальної поведінки інфікованих шкідливим програмним забезпеченням пристроїв Інтернету речей є моніторинг споживання енергії цими пристроями. Інфіковані пристрої часто демонструють підвищення енергоспоживання, що може бути індикатором зловмисної активності, такої як DDoS-атаки або криптомайнінг.

У статті представлено метод виявлення атак в інфраструктурі IoT, заснований на аналізі енергоспоживання пристроїв Інтернету речей, який враховує режими користувацьких налаштувань, пов'язані з енергоспоживанням пристроїв. Задля підвищення точності виявлення кібератак та локалізації шкідливого програмного забезпечення на пристроях застосовується аналіз послідовностей опкодів програмного забезпечення. Запропонований підхід надає можливість ефективно виявляти кібератаки, наприклад, DoS/DDoS, на рівні близько 99,88%, та локалізувати шкідливе програмне забезпечення на пристроях. Отже, моніторинг енергоспоживання розумних пристроїв опалення, вентиляції, кондиціонування повітря та інших пристроїв Інтернету речей є підходом до збільшення ефективності виявлення кібератак в інфраструктурі Інтернету речей.

Ключові слова: Інтернет речей, кібератака, DDoS, криптомайнінг, виявлення шкідливого програмного забезпечення, енергоспоживання, аналіз опкодів

Вступ. Інтернет речей та концепція «розумного дому» стали важливою частиною сучасного суспільства. З іншого боку, зростаюча кількість пристроїв Інтернету речей, які часто випускаються без будь-яких функцій безпеки, робить їх бажаною мішенню для кіберзлочинців [1, 2].

Незахищені пристрої Інтернету речей поповнюють ряди бот-мереж, які найчастіше використовуються для запуску DDoS-атак або як вузли виходу VPN. Криптомайнінг – ще один популярний спосіб монетизації скомпрометованих пристроїв Інтернету речей. Оскільки обмежена ємність акумуляторів смартфонів не дозволяє непомітно для користувача використовувати їх для отримання прибутку, розумні телевізори, телеприставки та інші пристрої Інтернету речей користуються популярністю серед кіберзлочинців. Майже будь-який розумний пристрій Інтернету речей, підключений до Інтернету, наприклад, лічильники газу, води та електроенергії, може стати об'єктом інтересу для кіберзлочинців [1].

Згідно зі звітами GSMA [3], у 2025 році кількість підключених пристроїв Інтернету речей сягає майже 25 млрд у всьому світі, а зі зростанням популярності Інтернету речей зростає й ризик кібератак.

Ефективне використання енергетичних ресурсів є ще одним із найважливіших завдань. Водночас майже третину загального споживання енергії складають певні втрати, тобто

енергія витрачається не за призначенням [4]. Зростання уваги до проблем енергоефективності та енергозбереження також сприяє розвитку концепції сучасного розумного дому. Крім того, якщо спочатку ця концепція полягала в об'єднанні давачів та розумних пристроїв через мережу з метою дистанційного моніторингу, доступу та контролю середовища та надання необхідних послуг користувачам, то на сучасному етапі вона також передбачає оптимальне використання енергії в будівлях, а також виявлення шкідливих програм та кібератак в інфраструктурі розумного дому.

Моніторинг споживання енергії пристроями Інтернету речей є одним з способів виявлення атак, що потребують значного споживання енергії [5], наприклад, DDoS та криптомайнінг. Методи виявлення атак на основі аналізу споживання енергії є більш надійними у випадках, коли ядро пристрою вже скомпрометовано, оскільки традиційні засоби захисту, як-от антивірусні програми, втрачають свою ефективність. Крім того, значна частина IoT-пристроїв не підтримує встановлення традиційного антивірусного програмного забезпечення через свою специфіку. Це пов'язано як з обмеженою обчислювальною потужністю, так і з закритою архітектурою операційної системи пристрою.

Аналіз наукових досліджень та постановка задачі. Сьогодні в наукових джерелах широко представлені різні підходи, спрямовані на забезпечення енергоефективності та енергозбереження в системі розумного дому [6-12]. У [13] зазначається, що в останні роки основним напрямком політики енергоефективності стало сприяння використанню більш ефективних приладів та компонентів. Однак, управління домашньою автоматизацією відіграє важливу роль в ефективному та сталому функціонуванні: (1) шляхом виявлення та усунення втрат енергії; (2) шляхом використання енергії лише в потрібній кількості, місці та лише тоді, коли вона потрібна; (3) шляхом здійснення правильного контролю функціонального рівня системи для правильного застосування в потрібному місці.

Сьогодні також існує дефіцит операційних систем, які б забезпечували можливість інтеграції пристроїв, що складають середовище розумного дому. Проблема впливає з того, що розумні пристрої базуються на модулях самообслуговування та використовують незалежні IoT-платформи, розроблені різними виробниками. Це призводить до необхідності керувати кожним пристроєм окремо, що знижує енергоефективність будинку та збільшує обсяг трафіку в мережі. Для вирішення цієї проблеми в [14] запропоновано інтегровану систему керування, яка об'єднує IoT-пристрої в єдину систему.

У [15] проведено аналіз переваг та ризиків технологій розумного дому з різних точок зору. Одним із важливих ризиків є недостатня увага розробників у сфері технологій розумного дому до заходів щодо підвищення довіри споживачів до безпеки та конфіденційності даних.

У [16] розглянуто різні підходи до інтелектуального керування домашніми системами з метою зменшення споживання енергії. Одним із таких підходів є випереджувальне керування (або керування з прямим зв'язком). Така система безпосередньо компенсує фактори перешкод, такі як зовнішня температура, вітер, сонячна радіація, внутрішнє теплопостачання, шляхом вимірювання таких факторів у режимі реального часу для вжиття відповідних заходів на основі відомих параметрів.

Іншим підходом є прогнозне керування на основі моделей [16], яке є структурованим підходом, що передбачає майбутню поведінку системи на основі моделей та відповідно коригує систему. Нечітке логічне керування не вимагає складної математичної моделі і може базуватися безпосередньо на якісних знаннях. Недоліком цього підходу є складність визначення оптимальних правил та функцій належності для таких систем [16].

Ще одним відомим підходом є штучні нейронні мережі, які широко використовуються для моделювання та прогнозування споживання енергії в будівлях. Штучні нейронні мережі здатні моделювати нелінійні процеси, постійно адаптуючись до нових даних та навчаючись на цих даних для вирішення складних проблем [16].

Також відомі гібридні підходи, засновані на використанні нечіткої логіки та штучних нейронних мереж, що поєднують переваги обох підходів – імітацію людської логіки та

здатність до навчання. Адаптивні нейронечіткі системи використовують алгоритми навчання нейронних мереж для налаштування функцій належності в нечіткій системі. У системі керування на основі агентів, які є віртуальними або фізичними модулями, агенти взаємодіють з навколишнім середовищем, сприймаючи та впливаючи на параметри за допомогою штучного інтелекту [16]. Такі системи здатні збалансувати споживання енергії, вартість та комфорт, вимірюючи та взаємодіючи з навколишнім середовищем, а також керуючи системами опалення, вентиляції та кондиціонування повітря й електроприладами.

У дослідженні [17] проаналізовано відомі системи енергоменеджменту в будинках з метою визначення ключових відмінностей у їхній функціональності та якості, а також визначено можливості для енергозбереження (як поведінкові, так і експлуатаційні). Також зазначається, що в багатьох випадках потенційні переваги, пов'язані зі зручністю, комфортом або безпекою, можуть обмежувати впровадження сценаріїв енергозбереження.

Також відомий ряд підходів, заснованих на моніторингу споживання енергії пристроями Інтернету речей, призначених для виявлення кібератак. У роботі [18] було кількісно досліджено вплив DDoS-атак на пристрої Інтернету речей та на їх споживання енергії, а також проаналізовано основні причини різних типів реакції цих пристроїв.

У [19] було представлено метод на основі машинного навчання, який дозволяє виявляти атаки програм-вимагачів шляхом моніторингу моделей споживання енергії різними процесами пристроїв Android.

У статті [20] запропоновано динамічний метод виявлення шкідливого програмного забезпечення для платформи Android. Цей метод використовує множину з 38 ознак, пов'язаних з енергоспоживанням, які належать до трьох різних категорій: таких як процесор, пам'ять та мережа, що може свідчити про аномальне споживання енергії батареї.

У статті [21] основна увага приділяється виявленню шкідливого програмного забезпечення на основі зібраних даних про споживання енергії та мережний трафік. З цією метою було застосовано 7 ознак, що базуються на енергоспоживанні, та 18 ознак, що базуються на мережному трафіку.

У роботі [22] також запропоновано фреймворк для виявлення атак на IoT, заснований на аналізі споживання енергії. Система обробляє рівень споживання енергії пристроями IoT та класифікує атаки за типом (не лише кібератаки, а й фізичні атаки). В роботі запропоновано двоетапну стратегію: застосування короткого часового вікна для грубого виявлення атаки та довгого часового вікна для підвищення точності виявлення атаки.

Разом з тим у статті [5] було проаналізовано відомі підходи виявлення шкідливого програмного забезпечення та кібератак на основі аналізу споживання енергії та зроблено висновок, що ці підходи не застосовні до таких пристроїв, як, наприклад, смартфони. Це пов'язано з тим, що типове споживання енергії такими пристроями на практиці досить сильно варіюється, зокрема, через непередбачувану взаємодію користувача та середовища. Відповідно, такі особливості функціонування призводять до великої кількості хибних тривог. Також були проведені емпіричні тести, які показали, що додаткова потужність, що споживається як штучними, так і реальними шкідливими програмами, занадто мала, щоб її можна було виявити з врахуванням середніх показників помилок сучасних вимірювальних інструментів. Однак було зазначено, що такі атаки, як DDoS, можна виявити, аналізуючи споживання енергії подібними пристроями.

Моніторинг споживання енергії пристроями Інтернету речей не може дати відповіді на питання щодо локалізації шкідливого програмного забезпечення як джерела кібератак. Одним з можливих підходів до локалізації шкідливого програмного забезпечення є аналіз опкодів програм.

Так, у [23] для виявлення програм-вимагачів запропоновано підхід, заснований на аналізі послідовностей N-грам опкодів. Для вилучення N-грам ознак обчислюється значення TF-IDF (term frequency – inverse document frequency, частота терма – обернена частота документа) для кожної з них. Зі значень TF N-грам ознак будуються вектори ознак, які обробляються методами машинного навчання для класифікації програм-вимагачів.

У [24] представлено метод на основі глибокого навчання для виявлення шкідливого програмного забезпечення в Internet Of Battlefield Things (IoBT, Інтернет речей на полі бою), який використовує покласовий відбір послідовностей опкодів як ознаки для завдання класифікації. Опкоди перетворюються у векторний простір, і для кожного зразка створюється граф ознак. Для класифікації шкідливих та легітимних програм було застосовано метод глибокого навчання у просторі власних значень.

У статті [25] було застосовано поєднання алгоритму видобування послідовних шаблонів з методами машинного навчання для виявлення послідовностей опкодів шкідливих IoT-застосунків, які зустрічаються найбільш часто.

У [26] запропоновано метод багатовимірної навчання, який використовує множину представлень, включаючи опкоди, байткоди, інформацію заголовка, дозволи, наміри зловмисника та виклики API для виявлення шкідливого програмного забезпечення. З метою оптимізації виявлення в різних середовищах запропонована система автоматично призначає різні ваги цим представленням.

У статті [27] запропоновано метод виявлення шкідливого програмного забезпечення, заснований на аналізі опкодів за допомогою еволюційного алгоритму. Згідно з цим підходом, мітка підозрілого екземпляра визначається на основі порівняння його графа з графами, отриманими для кожного сімейства шкідливих та легітимних програм.

Незважаючи на велику кількість відомих методів виявлення шкідливих програм та запобігання кібератакам, пристрої Інтернету речей все ще вразливі та зазнають широкого спектру кібератак та їхніх фінансових та репутаційних наслідків. Тому існує потреба в розробці нових підходів до виявлення шкідливих програм та кібератак в Інтернеті речей.

Метод виявлення кібератак в мережах Інтернету речей на основі аналізу енергоспоживання. Запропонований метод виявлення кібератак в IoT використовує аналіз енергоспоживання пристроїв IoT, а також застосовує аналіз послідовностей опкодів програмного забезпечення для підвищення точності виявлення та локалізації шкідливого програмного забезпечення на пристроях.

Для ефективного формування профілів енергоспоживання IoT-пристроїв необхідно враховувати різні режими користувацьких налаштувань (позначимо як user preference modes, UPM), пов'язані з енергоспоживанням систем HVAC (опалення, вентиляція та кондиціонування повітря), освітленням і функціонуванням різних IoT-пристроїв. Нехай множина режимів користувацьких уподобань для певного IoT-пристрою позначається як

$$P_d = \{p_i\}_{i=1}^{N_p}, \quad (1)$$

де d – певний IoT-пристрій, $d \in D$, $D = \{d_i\}_{i=1}^L$ – множина IoT-пристроїв у IoT-мережі, L – кількість IoT-пристроїв у мережі;

$p_i \in \{\text{"very low"}, \text{"low"}, \text{"normal"}, \text{"high"}, \text{"very high"}\}$, визначає пов'язаний із споживанням енергії UPM стосовно температури, освітлення, вологості, якості повітря тощо, а також функціонування інших IoT-пристроїв з множини D ;

N_p – кількість UPM для певного пристрою Інтернету речей, $N_p \geq 1$.

Також визначимо функцію контролю споживання енергії φ , яка підтримує споживання енергії IoT-пристроєм відповідно до заданого UPM як

$$\varphi: \{d \mid n_d \neq n_{d,p}\} \rightarrow n_{d,p}, \quad (2)$$

де n_d – поточне споживання енергії IoT-пристроєм;

$n_{d,p}$ – споживання енергії IoT-пристроєм d у певному режимі налаштувань користувача p .

Запропонований метод складається з двох етапів: навчання та виявлення. У свою чергу, етап навчання включає дві складові: аналіз енергоспоживання та аналіз послідовностей опкодів.

Нижче представлено етапи навчання компонента виявлення на основі аналізу енергоспоживання:

1. Побудова, нормалізація та маркування профілів енергоспоживання IoT-пристроїв для різних режимів користувацьких уподобань за відсутності кібератак.
2. Побудова, нормалізація та маркування профілів енергоспоживання IoT-пристроїв для різних режимів користувацьких уподобань за наявності кібератак.
3. Створення промаркованих і немаркованих матриць даних профілів енергоспоживання IoT-пристроїв.
4. Напівкероване навчання нечіткого класифікатора *c-means* з використанням промаркованої матриці даних профілів енергоспоживання IoT-пристроїв.
5. Тестування нечіткого класифікатора *c-means* за допомогою немаркованої матриці даних профілів енергоспоживання IoT-пристроїв.
6. Оцінка ефективності аналізу енергоспоживання.

Як зазначалося вище, для підвищення точності виявлення атак на основі аналізу енергоспоживання та для локалізації шкідливого програмного забезпечення застосовується аналіз послідовностей опкодів. Етапи навчання компонента виявлення на основі аналізу послідовностей опкодів наведено нижче:

1. Витягнення асемблерного представлення зі шкідливих та легітимних двійкових виконуваних файлів IoT-пристроїв.
2. Пошук максимальних послідовних патернів (*maximal sequential patterns, MSP*) опкодів у асемблерних представленнях двійкових виконуваних файлів.
3. Відбір MSP для формування векторів ознак.
4. Обчислення релевантності для кожного з MSP.
5. Побудова та маркування векторів ознак релевантності MSP опкодів для кожного асемблерного представлення двійкового виконуваного файлу.
6. Побудова промаркованої та немаркованої матриці даних векторів ознак релевантності MSP опкодів.
7. Напівкероване навчання нечіткого класифікатора *c-means* з використанням промаркованої матриці даних векторів ознак релевантності MSP опкодів.
8. Тестування нечіткого класифікатора *c-means* за допомогою немаркованої матриці даних векторів ознак релевантності MSP опкодів.
9. Оцінювання ефективності аналізу послідовностей опкодів.

На етапі виявлення запропонованого методу за допомогою навченого класифікатора аналізуються профілі енергоспоживання IoT-пристроїв. Якщо IoT-пристрій має аномально високе енергоспоживання, це може свідчити про здійснення кібератак. Однак моніторинг споживання енергії IoT-пристроями не дає відповіді на питання локалізації шкідливого програмного забезпечення на цьому пристрої, яке є джерелом кібератаки. Тому необхідно проаналізувати підозріле програмне забезпечення на IoT-пристрої. З цією метою в асемблерному представленні підозрілого двійкового виконуваного файлу здійснюється аналіз послідовностей опкодів для виявлення максимальних послідовних патернів (MSP). Для отриманих MSP обчислюється їх релевантність, будуються вектори ознак для підозрілого програмного забезпечення, а потім ці вектори аналізуються за допомогою навченого класифікатора. Схема методу представлена на рис. 1.

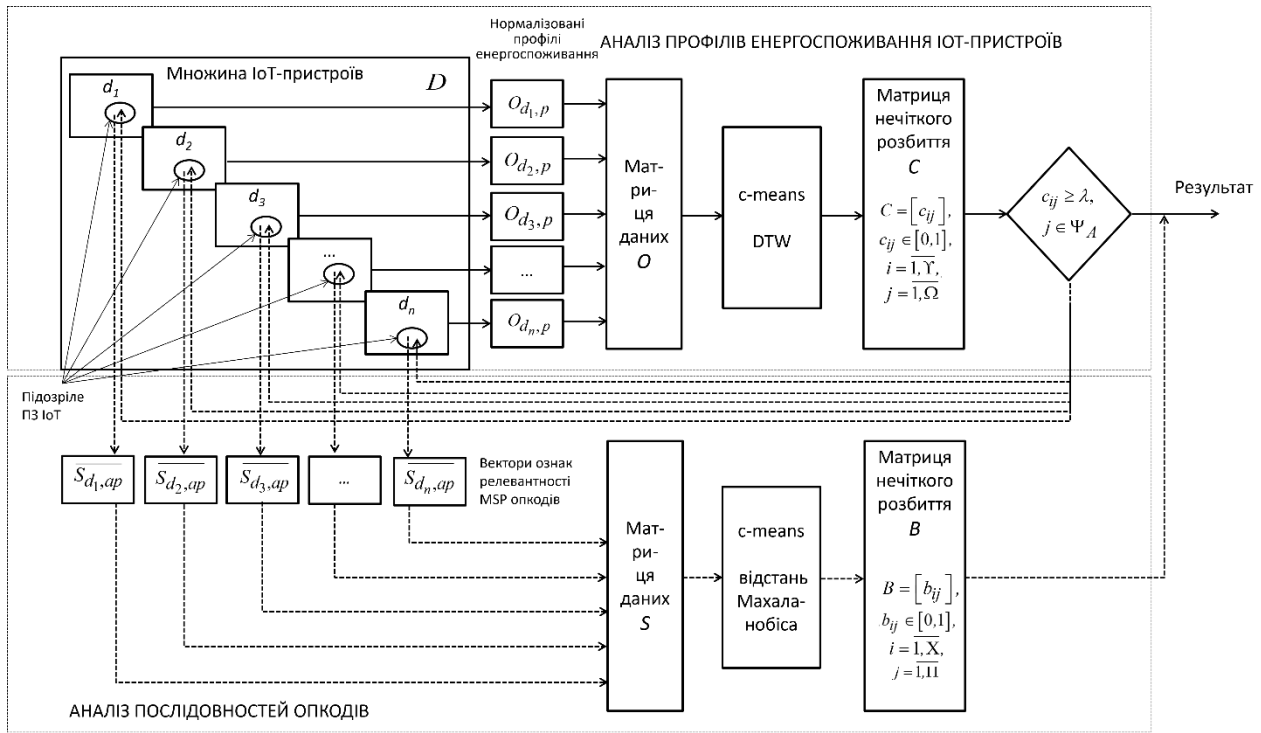


Рисунок 1 – Схема методу виявлення кібератак в мережах Інтернету речей на основі аналізу енергоспоживання

Розглянемо більш детально основні кроки методу.

Побудова профілів енергоспоживання. На етапі навчання вимірюється споживання енергії кожним пристроєм IoT у мережі IoT для різних UPM за відсутності кібератак в межах певного інтервалу та через рівні підінтервали часу. На основі цих вимірювань формується множина профілів енергоспоживання IoT-пристроїв $N_{d,p}$, частина з яких позначена як «нормальні» профілі та внесена до маркованої матриці даних D_l , а решта внесені до немаркованої матриці даних D_{unl} (рис. 2).

Опишемо профіль енергоспоживання IoT-пристрою за відсутності кібератак, враховуючи множину режимів уподобань користувача (UPM), як

$$N_{d,p} = (n_{d,p,i})_{i=1}^K, \quad (3)$$

де $n_{d,p,i}$ – нормалізоване вимірювання споживання енергії IoT-пристрою d в певний момент часу за відсутності кібератак для режиму функціонування пристрою, який визначається уподобаннями користувача, $p, n_{d,p,i} \in [0,1]$, де 0 вказує на відсутність споживання енергії, а 1 – на максимальне споживання енергії за відсутності кібератак; K – кількість вимірювань у часовому інтервалі.

Також необхідно побудувати профілі енергоспоживання IoT-пристроїв за наявності різних типів кібератак з урахуванням UPM. Аналогічним чином вимірюється споживання енергії IoT-пристроями для різних UPM в межах певного інтервалу та через рівні підінтервали часу за наявності кібератак. На основі цих вимірювань формується множина профілів енергоспоживання IoT-пристроїв за наявності кібератак $A_{d,p,t}$, частина з яких позначається як профілі енергоспоживання для певного типу кібератак Інтернету речей та вноситься до промаркованої матриці даних D_l , а решта – до немаркованої матриці даних D_{unl} (рис. 2).

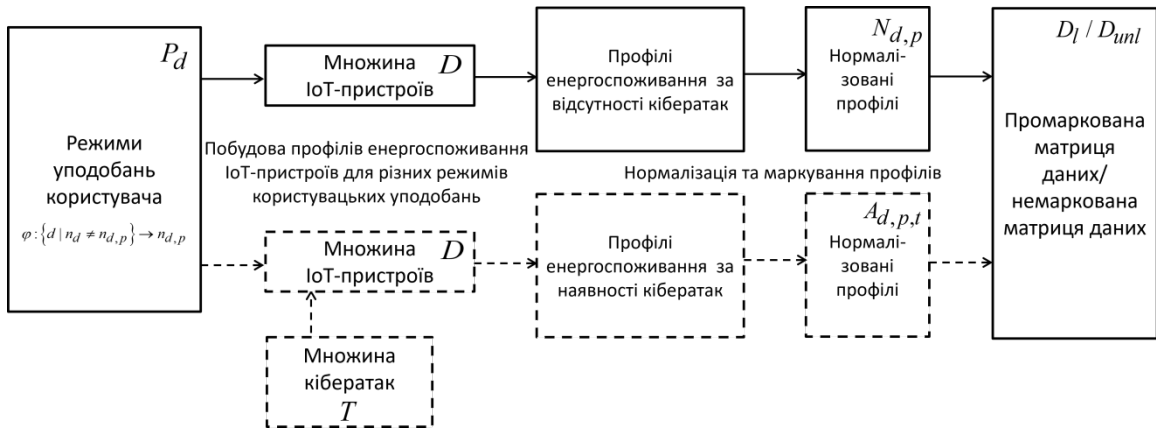


Рисунок 2 – Побудова профілів енергоспоживання IoT-пристроїв для різних UPM за відсутності та за наявності кібератак

Аналогічно опишемо множину профілів енергоспоживання IoT-пристроїв за наявності кібератак, враховуючи множину UPM, як

$$A_{d,p,t} = (a_{d,p,t,i})_{i=1}^K, \quad (4)$$

де $a_{d,p,t,i}$ – нормалізоване вимірювання споживання енергії IoT-пристроєм у певний момент часу за наявності певних типів кібератак, $a_{d,p,t,i} \in [0,1]$, де 0 вказує на відсутність споживання енергії, а 1 – на максимальне споживання енергії за наявності кібератак; $t \in T$ – тип кібератаки Інтернету речей, T – множина типів кібератак Інтернету речей; K – кількість вимірювань у часовому інтервалі.

На основі одержаних профілів виконується напівкероване навчання нечіткого класифікатора c-means з використанням промаркованої матриці даних D_l профілів енергоспоживання $N_{d,p}$ і $A_{d,p,t}$.

Для оцінки ефективності виявлення кібератак на основі енергоспоживання здійснюється тестування нечіткого класифікатора c-means за допомогою немаркованої матриці даних D_{unl} .

Побудова векторів ознак релевантності MSP опкодів. З метою аналізу послідовностей опкодів на етапі навчання з легітимних та шкідливих зразків двійкових виконуваних файлів IoT-пристроїв витягуються їх асемблерні представлення. Із цих представлень шляхом застосування алгоритм пошуку послідовних шаблонів витягуються MSP опкодів.

Для кожного MSP розраховується IDF (Inverse Document Frequency, обернена частота документа), яке зменшує вагу часто використовуваних MSP:

$$IDF(MSP, Z) = \log \frac{|Z|}{|\{z_i \in Z \mid MSP \in z_i\}|}, \quad (5)$$

де $|Z|$ – загальна кількість виконуваних файлів $z \in Z$, $Z = Z_b \cup Z_m$, де Z_b – множина легітимного програмного забезпечення Інтернету речей, Z_m – множина шкідливого програмного забезпечення Інтернету речей;

$|\{z_i \in Z \mid MSP \in z_i\}|$ – кількість виконуваних файлів Z у множині Z , в яких зустрічається MSP .

Щоб визначити місце MSP опкодів у векторі ознак, MSP сортуються за зростанням значення $IDF(MSP, Z)$:

$$R = (IDF(MSP_i, Z))_{i=1}^{N_R}, \quad IDF(MSP_i, Z) < IDF(MSP_{i+1}, Z), \quad (6)$$

де N_R – загальна кількість різних MSP.

Для оцінки релевантності MSP для кожного MSP розраховуються значення зваженої частоти терма (Weighted Term Frequency, WTF) [28]. WTF визначається як результат

зважування частоти терма (TF) відповідно до релевантності кожного опкоду. O та обчислюються як добуток частоти послідовності й ваги кожного опкоду O у послідовності MSP:

$$WTF(MSP, z) = TF(MSP, z) \times \prod_{o \in MSP} \frac{W(o)}{100}, \quad (7)$$

де $W(o)$ – обчислена вага опкоду o на основі приросту взаємної інформації;

$TF(MSP, z)$ – метрика частоти MSP у програмному забезпеченні.

Частота терму, $TF(MSP, z)$, надає оцінку важливості MSP у виконуваному файлі програмного забезпечення і може бути розрахована наступним чином:

$$TF(MSP, z) = \frac{f_{MSP, z}}{\sum_{MSP' \in Z} f_{MSP', z}}, \quad (8)$$

де $f_{MSP, z}$ – кількість появ MSP у виконуваному файлі z ; $\sum_{MSP' \in Z} f_{MSP', z}$ – загальна кількість послідовностей опкодів у виконуваному файлі z .

Взаємна інформація $I(F; \Psi)$, на якій ґрунтується розрахунок, є мірою статистичної залежності двох змінних. У цьому випадку ними є окремий опкод o і факт того, чи є програмне забезпечення шкідливим, чи ні.

$$I(F; \Psi) = \sum_{\psi \in \Psi} \sum_{f \in F} p(f, \psi) \log \left(\frac{p(f, \psi)}{p(f) \times p(\psi)} \right), \quad (9)$$

де F – частота опкоду;

Ψ – клас файлу;

$p(f, \psi)$ – функція спільного розподілу ймовірності F і Ψ ;

$p(f)$ і $p(\psi)$ – функції розподілу граничних ймовірностей F і Ψ .

З отриманих для MSP значень WTF для кожного двійкового файлу будується вектор ознак релевантності MSP опкодів. Вектори, довжина яких більша за медіанну довжину. H усіх отриманих векторів, обрізаються. Якщо довжина вектора менша за медіанну довжину, він доповнюється нулями.

Позначимо вектор ознак релевантності MSP опкодів як

$$\overline{s_{d, ap}} = (s_{d, ap, i})_{i=1}^H, \quad (10)$$

де $s_{d, ap, i}$ – релевантність MSP опкодів програмного забезпечення IoT;

H – кількість MSP опкодів програмного забезпечення IoT.

Частина побудованих векторів, позначена як «легітимна» або «шкідлива» відповідно, заноситься до промаркованої матриці даних W_l , а решта – до немаркованої матриці даних W_{unl} (рис. 3).

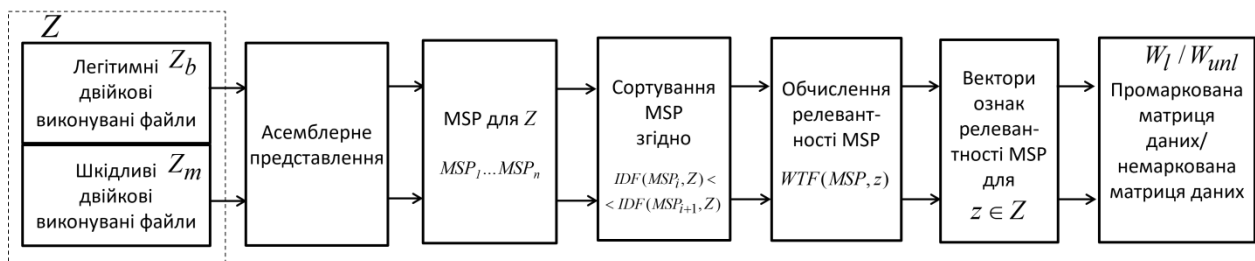


Рисунок 3 – Побудова векторів ознак релевантності MSP опкодів

Класифікація даних. Для класифікації даних застосовано напівкеровану нечітку кластеризацію c-means. Перевага нечіткої кластеризації полягає у відсутності жорсткої вимоги однозначного віднесення об'єктів до кластерів. Це стає можливим завдяки використанню функцій належності, що приймають значення в інтервалі $[0, 1]$. Такий підхід

дозволяє підвищити точність та повноту результатів кластеризації, особливо для об'єктів, що розташовані на межах кластерів.

Застосування напівкеруваного навчання надає можливість уточнити початкові центри кластерів, що покращує якість результатів кластеризації. Початкові центри кластерів визначалися на основі навчальної вибірки, обсяг якої становив 10% від даних, зібраних для аналізу.

Як об'єкти кластеризації використовувалися профілі енергоспоживання IoT-пристроїв. Замість евклідової відстані (яка застосовується в базовому алгоритмі c-means) для кластеризації профілів енергоспоживання було використано динамічне вирівнювання часових послідовностей (dynamic time warping, DTW). Використання евклідової відстані має суттєвий недолік: якщо два часові ряди однакові, але один з них трохи зміщений у часі, то евклідова відстань може призводити до помилкового висновку, що ряди відрізняються один від одного. Алгоритм DTW був застосований для того, щоб подолати цей недолік і забезпечити вимірювання відстані між рядами, усуваючи зміщення на часовій шкалі.

Результатом кластеризації профілів енергоспоживання IoT-пристроїв є матриця нечіткого розбиття C , де кожен елемент матриці c_{ij} визначає ступінь приналежності i -го елемента (профілю енергоспоживання IoT-пристрою) до j -го кластера: $C = [c_{ij}]$, $c_{ij} \in [0,1]$, $i = \overline{1, Y}$, $j = \overline{1, \Omega}$, $\sum_{j=1, \Omega} c_{ij} = 1$, де Y – кількість профілів енергоспоживання, Ω –

кількість кластерів. Отже, кожен об'єкт кластеризації з певним ступенем приналежності відноситься до кожного з Ω кластерів, що дозволяє визначити нормальне споживання енергії (певний режим користувача) або підвищене, яке може вказувати на атаку.

Для класифікації векторів ознак релевантності MSP опкодів замість евклідової відстані використовувалася відстань Махаланобіса. Вона дозволяє формувати кластери у вигляді гіпереліпсоїдів з осями, орієнтованими в довільних напрямках, що дає змогу враховувати можливу наявність викидів у даних, тобто результатів спостережень, що виділяються із загальної вибірки.

Результатом кластеризації векторів ознак релевантності MSP опкодів є нечітка матриця розбиття B , де кожен її елемент b_{ij} визначає ступінь приналежності i -го елемента множини об'єктів кластеризації до j -го кластера: $B = [b_{ij}]$, $b_{ij} \in [0,1]$, $i = \overline{1, X}$, $j = \overline{1, \Pi}$, $\sum_{j=1, \Pi} b_{ij} = 1$, де X –

кількість векторів ознак релевантності MSP опкодів, Π – кількість кластерів. Таким чином, кожен вектор ознак з певним ступенем приналежності належить до кожного з Π кластерів. Кожен кластер позначає легітимне програмне забезпечення або певний тип шкідливого програмного забезпечення.

Для віднесення об'єкта до кластера використовується порогове значення належності λ . Якщо максимальний ступінь належності об'єкта кластеризації перевищує поріг, тоді об'єкт належить до відповідного кластера.

Також позначимо множину всіх кластерів як $\Psi = \Psi_N \cup \Psi_A$, де Ψ_N є підмножиною кластерів, що відповідають легітимним об'єктам, Ψ_A є підмножиною кластерів, що відповідають шкідливим об'єктам (рис. 1).

Експериментальні результати. Для оцінки ефективності запропонованого підходу було проведено низку експериментів. Як цільову платформу Інтернету речей для експериментів було обрано платформу ARM, оскільки вона є однією з найбільш поширених платформ Інтернету речей. Було використано різноманітні IoT-пристрої на базі ARM (такі як смарт-телевізори, відеокамери та маршрутизатори). Також було використано 284 зразки легітимного програмного забезпечення [29] та 297 зразків шкідливого програмного забезпечення [30], включно з 91 поліморфним зразком шкідливого програмного забезпечення, згенерованим за допомогою інструменту з відкритим кодом для створення поліморфного шкідливого ПЗ [31].

IoT-пристрої, що використовувалися в експериментах, були інфіковані шкідливим програмним забезпеченням та використовувалися для здійснення DDoS-атак на ціль в ізольованій мережі. Під час експериментів були отримані профілі енергоспоживання IoT-пристроїв за нормальних умов експлуатації, а також під час здійснення ними кібератак. Кожен профіль енергоспоживання був отриманий шляхом вимірювань через 0,5 с протягом 3 хвилин, коли IoT-пристрій здійснював атаку, і коли він працював у звичайному режимі. Загалом було побудовано 1253 профілі енергоспоживання як за наявності атак, так і за нормального функціонування IoT-пристроїв.

Також зі зразків шкідливого програмного забезпечення, яке здійснювало атаки, були видобуті послідовності опкодів. З цією метою зразки програмного забезпечення були дизасембльовані за допомогою IDA Pro [32] та був використаний алгоритм видобутку послідовних шаблонів на основі хешів (hash-based partition sequential pattern mining algorithm, HPSPM) [33].

Частина одержаних даних (близько 10%) була використана для навчання, а решта – як тестові дані для оцінки ефективності запропонованого підходу. Для класифікації шкідливих зразків були застосовані класифікатори Support Vector Machine (SVM), K Nearest Neighbor (KNN), Decision Tree, Random Forest та напівкерований нечіткий c-means.

Для оцінки ефективності запропонованого підходу були застосовані наступні показники. Точність (ассигасу) – це статистичний показник, який визначає частку правильних прогнозів (як істинно позитивних, так і істинно негативних) серед загальної кількості досліджених випадків:

$$ACC = \frac{TP + TN}{TP + TN + FP + FN}, \quad (11)$$

де TP (істинно позитивний результат) – правильно класифіковані зразки шкідливого програмного забезпечення;

TN (істинно негативний) – правильно класифіковані зразки, які є легітимними;

FN (хибно негативні) – шкідливі зразки, помилково класифіковані як легітимні;

FP (хибно позитивні) – легітимні зразки, помилково класифіковані як шкідливі.

Іншим застосованим показником точності є F_1 -міра (або збалансована F -оцінка, F_1 -оцінка), що визначається як гармонійне середнє точності та повноти:

$$F_1 = 2 \times \frac{PREC \times REC}{PREC + REC}, \quad (12)$$

$$\text{де } PREC = \frac{TP}{TP + FP}, \quad REC = \frac{TP}{TP + FN}.$$

Експериментальні результати представлені в табл. 1 і 2. Результати експериментів показали високу ефективність виявлення кібератак на основі аналізу енергоспоживання (табл. 1).

Таблиця 1

Експериментальні результати: точність та значення F_1 -міри для виявлення кібератак Інтернету речей на основі аналізу енергоспоживання

Класифікатор	TP	TN	FN	FP	ACC	F_1
Decision Tree	1235	1239	18	14	98.72	98.72
K Nearest Neighbor	1236	1241	17	12	98.84	98.84
Random Forest	1242	1247	11	6	99.32	99.32
Support Vector Machine	1248	1249	5	4	99.64	99.64
Semi-Supervised Fuzzy C-Means clustering	1251	1252	2	1	99.88	99.88

Водночас, як видно з табл. 2, аналіз послідовностей опкодів підозрілого програмного забезпечення дає змогу з високою ефективністю локалізувати програму на IoT-пристрої, що є джерелом кібератаки. Як видно з наведених експериментальних результатів, найвищої

ефективності було досягнуто з використанням нечіткого класифікатора c-means з напівкерованим навчанням.

Таблиця 2

Експериментальні результати: точність та значення F-міри для локалізації шкідливого програмного забезпечення шляхом аналізу послідовностей опкодів

Класифікатор	TP	TN	FN	FP	ACC	F ₁
Random Forest	285	276	12	8	96.56	96.61
Decision Tree	292	278	5	6	98.11	98.15
K Nearest Neighbor	293	281	4	3	98.80	98.82
Support Vector Machine	295	280	2	4	98.97	98.99
Semi-Supervised Fuzzy C-Means	296	283	1	1	99.66	99.66

Висновки. Отже, враховуючи, що високе споживання енергії IoT-пристроєм може свідчити про здійснення кібератак, було запропоновано новий метод їх виявлення на основі аналізу енергоспоживання. Відповідно до методу, для виявлення атак будуються та аналізуються профілі енергоспоживання IoT-пристроїв з урахуванням режимів уподобань користувачів, пов'язаних зі споживанням енергії. Для локалізації шкідливого програмного забезпечення на IoT-пристроях аналізуються послідовності опкодів підозрілих двійкових файлів. Для цього видобуваються їх максимальні послідовні патерни (MSP), обчислюється їх релевантність, і будуються вектори ознак релевантності MSP опкодів для кожного асемблерного представлення. З метою класифікації даних застосовано напівкеровану нечітку кластеризацію c-means.

Експериментальні результати показують, що запропонований підхід дає змогу ефективно виявляти атаки, зокрема DoS/DDoS, на рівні близько 99,88%, та локалізувати шкідливе програмне забезпечення на пристроях Інтернету речей з точністю близько 99,66%.

ЛІТЕРАТУРА:

1. Trend Micro. Inside the Smart Home: IoT Device Threats and Attack Scenarios. URL: <https://www.trendmicro.com/vinfo/it/security/news/internet-of-things/inside-the-smart-home-iot-device-threats-and-attack-scenarios>.
2. McAfee Labs Threats Report. URL: <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-nov-2020.pdf>.
3. Global System for Mobile Communications. URL: <https://www.gsma.com/>
4. U.S. Energy Information Administration (EIA). International Energy Outlook, 2019. URL: <https://www.eia.gov/outlooks/ieo>.
5. J. Hoffmann, S. Neumann, T. Holz, Mobile malware detection based on energy fingerprints – a dead end?. In International Workshop on Recent Advances in Intrusion Detection. Springer, Berlin, Heidelberg (2013), pp.348-368.
6. A. R. Al-Ali, I. A. Zuolkernan, M. Rashid, R. Gupta & M. Alikarar, A smart home energy management system using IoT and big data analytics approach. IEEE Transactions on Consumer Electronics. 2017, Vol. 63(4), pp. 426-434.
7. M. S. Hossain, M. A. Rahman & G. Muhammad, Cyber-physical cloud-oriented multi-sensory smart home framework for elderly people: An energy efficiency perspective. Journal of Parallel and Distributed Computing. 2017, Vol. 103, pp. 11-21.
8. M. Isnén, S. Kurniawan & E. Garcia-Palacios, A-SEM: An adaptive smart energy management testbed for shiftable loads optimisation in the smart home. Measurement. 2020, Vol. 152, 107285.
9. M. A. Paredes-Valverde, G. Alor- Hernández, J. L. García- Alcaráz, M. D. P. Salas- Zárate, L. O. Colombo-Mendoza & J. L. Sánchez-Cervantes, IntelliHome: An internet of things- based system for electrical energy saving in smart home environment. Computational Intelligence. 2020, Vol. 36 (1), pp. 203-224.

- 10.A. De Paola, P. Ferraro, G. L. Re, M. Morana & M. Ortolani, A fog-based hybrid intelligent system for energy saving in smart buildings. *Journal of Ambient Intelligence and Humanized Computing*. 2020, Vol. 11 (7), pp. 2793-2807.
- 11.M. Killian, M. Zauner & M. Kozek, Comprehensive smart home energy management system using mixed-integer quadratic-programming. *Applied energy*. 2018, Vol. 222, pp. 662-672.
- 12.I. Machorro-Cano, G. Alor-Hernández, M. A. Paredes-Valverde, L. Rodríguez-Mazahua, J. L. Sánchez-Cervantes & J. O. Olmedo-Aguirre, HEMS-IoT: A big data and machine learning-based smart home system for energy saving. *Energies*. 2020, Vol. 13 (5), 1097.
- 13.V. Fabi, G. Spiglientini & S. P. Corgnati, Insights on smart home concept and occupants' interaction with building controls. *Energy Procedia*. 2017, Vol. 111, pp. 759-769.
- 14.H. Jo, Y. I. Yoon, Intelligent smart home energy efficiency model using artificial TensorFlow engine. *Human-centric Computing and Information Sciences*. 2018, Vol. 8 (1), pp. 1-18.
- 15.C. Wilson, T. Hargreaves, R. Hauxwell-Baldwin, Benefits and risks of smart home technologies. *Energy Policy*. 2017, Vol. 103, pp. 72-83.
- 16.L. C. Felius, F. Dessen & B. D. Hrynyszyn, Retrofitting towards energy-efficient homes in European cold climates: a review. *Energy Efficiency*. 2020, Vol. 13 (1), pp. 101-125.
- 17.R. Ford, M. Pritoni, A. Sanguinetti & B. Karlin, Categories and functionality of smart home technology for energy management. *Building and environment*. 2017, Vol. 123, pp. 543-554.
- 18.B. Tushir, Y. Dalal, B. Dezfouli & Y. Liu, A Quantitative Study of DDoS and E-DDoS Attacks on WiFi Smart Home Devices. *IEEE Internet of Things Journal*, 2020.
- 19.A. Azmoodeh, A. Dehghantanha, M. Conti & K. K. R. Choo, Detecting crypto-ransomware in IoT networks based on energy consumption footprint. *Journal of Ambient Intelligence and Humanized Computing*. 2018, Vol. 9 (4), pp. 1141-1152.
- 20.F. Fasano, F. Martinelli, F. Mercaldo & A. Santone, Energy consumption metrics for mobile device dynamic malware detection. *Procedia Computer Science*. 2019, Vol. 159, pp. 1045-1052.
- 21.J. H. Jimenez, K. Goseva-Popstojanova, Malware detection using power consumption and network traffic data. In 2019 2nd International Conference on Data Intelligence and Security (ICDIS). IEEE (2019), pp. 53-59.
- 22.Y. Shi, F. Li, W. Song, X. Y. Li & J. Ye, Energy audition based cyber-physical attack detection system in IoT. In *Proceedings of the ACM Turing Celebration Conference-China (2019)*, pp. 1-5.
- 23.H. Zhang, X. Xiao, F. Mercaldo, S. Ni, F. Martinelli & A. K. Sangaiah, Classification of ransomware families with machine learning based on N-gram of opcodes. *Future Generation Computer Systems*. 2019, Vol. 90, pp. 211-221.
- 24.A. Azmoodeh, A. Dehghantanha & K. K. R. Choo, Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning. *IEEE transactions on sustainable computing*. 2018, Vol. 4 (1), pp. 88-95.
- 25.H. Darabian, A. Dehghantanha, S. Hashemi, S. Homayoun & K. K. R. Choo, An opcode-based technique for polymorphic Internet of Things malware detection. *Concurrency and Computation: Practice and Experience*. 2020, Vol. 32 (6), e5173.
- 26.H. Darabian, A. Dehghantanha, S. Hashemi, M. Taheri, A. Azmoodeh, S. Homayoun & R. M. Parizi, A multiview learning method for malware threat hunting: windows, IoT and android as case studies. *World Wide Web*. 2020, Vol. 23 (2), pp. 1241-1260.
- 27.F. Manavi, A. Hamzeh, A new approach for malware detection based on evolutionary algorithm. In *Proceedings of the Genetic and Evolutionary Computation Conference Companion (2019)*, pp.1619-1624.
- 28.I. Santos, F. Brezo, X. Ugarte-Pedrero & P. G. Bringas, Opcode sequences as representation of executables for data-mining-based unknown malware detection. *Information Sciences*. 2013, Vol. 231, pp. 64-82.
- 29.Packages Search for Linux and Unix. URL: <https://pkgs.org/>
- 30.VirusTotal. URL: <http://www.virustotal.com>
- 31.Obfuscator-for-ARM-disassembled-binary. URL: <https://github.com/darabian/Obfuscator-for-ARM-disassembled-binary>
- 32.Hex Rays. IDA Pro. URL: <https://www.hex-rays.com/products/ida/>
- 33.R. Millham, I. E. Agbehadji, H. Yang, Pattern Mining Algorithms. In *Bio-inspired Algorithms for Data Streaming and Visualization, Big Data Management, and Fog Computing*. Springer, Singapore (2021), pp. 67-80.

A METHOD AND ALGORITHMS FOR DETECTING CYBERATTACKS IN INTERNET OF THINGS NETWORKS BASED ON ENERGY CONSUMPTION ANALYSIS

A «Smart home» is a system for managing the essential life support processes of both small systems (commercial, office spaces, apartments, cottages) and large automated commercial and industrial complexes. An important task that the modern «Smart home» concept must address is preventing the spread of malicious software within the Internet of Things (IoT) infrastructure. Despite the vast number of developed methods for detecting and preventing cyberattacks, IoT devices are still extremely vulnerable and suffer a wide range of cyberattacks, which have both financial and reputational consequences. Therefore, there is a need to develop new approaches for detecting malicious software in the IoT infrastructure. One possible approach for detecting the anomalous behavior of malware-infected IoT devices is to monitor their energy consumption. Infected devices often exhibit an increase in energy consumption, which can be an indicator of malicious activity, such as DDoS attacks or cryptomining.

This article presents a method for detecting attacks in the IoT infrastructure based on the analysis of IoT device energy consumption, which takes into account user preference modes related to device energy consumption. To enhance the accuracy of cyberattack detection and the localization of malicious software on devices, an analysis of software opcode sequences is applied. The proposed approach provides the ability to effectively detect cyberattacks, such as DoS/DDoS, with an accuracy of approximately 99.88%, and to localize malicious software on devices. Thus, monitoring the energy consumption of smart heating, ventilation, air conditioning (HVAC) devices, and other IoT devices is an approach to increasing the effectiveness of cyberattack detection in the IoT infrastructure.

Keywords: Internet of Things, cyberattack, DDoS, cryptomining, malware detection, energy consumption, sequential pattern mining, opcode analysis

ПЕРЕДАВАЛЬНА ФУНКЦІЯ РОЗІМКНЕНОЇ СИСТЕМИ АВТОМАТИЧНОГО УПРАВЛІННЯ З ГІДРОПРИВОДОМ

У статті виведена передавальна функція системи автоматичного управління з гідроциліндрами в якості виконавчого пристрою. Необхідність отримання моделі пов'язана з синтезом одного з каналів системи.

Загальна система автоматичного управління містить декілька каналів управління. Систему побудовано для специфічного об'єкта. Це уніфікована стабілізаційна платформа нетипового вогневого засобу на високомобільній транспортній базі. Одним з завдань системи автоматичного управління є компенсація впливу від застосування вогневого засобу. Управління відбувається відповідно до математичної моделі об'єкту вогневий засіб – транспортний засіб. Синтез каналів зі зворотнім зв'язком, які присутні в системі, в роботі не розглядається. Основна увага приділяється моделюванню процесів у канал без зворотного зв'язку. Такий варіант побудови (каналу системи автоматичного управління) та вибір виконавчого пристрою обумовлений типом зовнішнього впливу на об'єкт управління (короткотривалий імпульс високої інтенсивності).

Математичне моделювання основних компонентів розімкненої системи: джерела сигналу управління, електромагнітного клапана та гідроциліндра проведено з урахуванням процесів, які відбуваються в елементах системи.

На основі передавальних функцій окремих компонент визначено загальну передавальну функцію системи (каналу управління). Додатково враховано інерційні характеристики, що виникають через масу рухомих частин (поршня, штока, навантаження), демпфуючі фактори та гідравлічну динаміку. В результаті отримано уточнену математичну модель системи автоматичного управління із гідроприводом, що відображає динамічні властивості системи з урахуванням реальних фізичних процесів.

Запропонований підхід може бути використаний для подальшого аналізу стійкості та якості керування гідроприводами в промислових і транспортних застосуваннях.

Ключові слова: канал управління, система автоматичного управління, передавальна функція, зворотній зв'язок, виконавчий пристрій, гідросистема, вогневий засіб, транспортна база.

Постановка задачі у загальному вигляді. Системи автоматичного управління (САУ) із гідроприводами широко застосовуються в промислових, транспортних і мехатронних комплексах, де необхідне регулювання положення [1], швидкості або зусилля виконавчих механізмів. Високі динамічні характеристики гідравлічних систем роблять їх незамінними у важких умовах експлуатації. Проте такі системи мають низку особливостей, які ускладнюють процес синтезу алгоритмів управління, зокрема: наявність нелінійних та інерційних ефектів у гідравлічному середовищі; залежність динаміки виконавчого механізму від гідродинамічних процесів у приводі; вплив параметрів клапанної апаратури та характеристик робочої рідини на загальну динаміку системи [2].

Ключовим етапом розробки ефективних алгоритмів управління є побудова адекватної математичної моделі, що описує динаміку об'єкта управління. У даній роботі поставлено задачу виведення передавальної функції САУ із гідроприводом, що дозволяє формалізувати залежність між впливом управління і вихідними координатами виконавчого пристрою.

Аналіз останніх досліджень і публікацій. Системи автоматичного управління з гідроприводами є об'єктом численних досліджень, спрямованих на підвищення їх ефективності, надійності та адаптивності до сучасних вимог. Останні публікації висвітлюють різні аспекти розвитку та вдосконалення таких систем.

В роботі [3] досліджується впровадження алгоритмів штучного інтелекту для прогнозованого технічного обслуговування гідравлічних систем, що підвищує їх надійність та продовжує термін служби обладнання. У статті [4] отримано математичну модель гідроциліндра та проаналізовано параметри, що суттєво впливають на динаміку роботи гідроциліндра у період його пуску. У роботі [5] було розроблено розрахункову схему автоматичного регулятора насоса змінної продуктивності, який забезпечує стабілізацію витрати та роботу насоса з постійною потужністю. Викладено методику динамічного синтезу електрогідравлічного слідкуючого приводу для забезпечення заданої швидкодії та форми перехідного процесу і точності позиціонування робочого органу [6].

У дослідженнях автоматичної системи регулювання рівня води проаналізовано об'єкт регулювання, умови його роботи та основні збурення. Сформульовано вимоги до системи автоматичного регулювання та вибрано принципи регулювання для покращення її властивостей [7].

Автоматизацію процесів керування технологічним обладнанням з гідроприводом обертального руху представлено в [8, 9], де розглянуто можливості розширення функціональних можливостей та покращення динамічних характеристик технологічного обладнання з гідроприводом обертального руху шляхом розробки та застосування САУ.

Метою статті є отримання передавальної функції системи автоматичного керування із гідроциліндром в якості виконавчого пристрою, з урахуванням основних динамічних характеристик її елементів. Це дозволить формалізувати математичну модель системи, провести аналіз її стійкості, динамічних властивостей та оцінити ефективності процесу управління.

Виклад основного матеріалу.

Загальна структура системи управління об'єктом вогневий засіб – транспортний засіб (ВЗ-ТЗ) представлена на рис.1. Блок датчиків об'єднує в собі вимірювальні та задаючі датчики всіх контурів керування САУ (інерційні вимірювачі, приймач супутникових сигналів системи GPS, статичні та динамічні датчики, датчики кутів, тощо).

В якості бортового обчислювача використано мікропроцесорну систему, в пам'яті якої закладено математичні моделі різних типів ВЗ та коливальних властивостей підресорної частини ТЗ.

На систему покладається два основних завдання, а саме: приведення об'єкту ТЗ-ВЗ в бойову готовність та компенсація збурювальної дії ВЗ на транспортну базу.

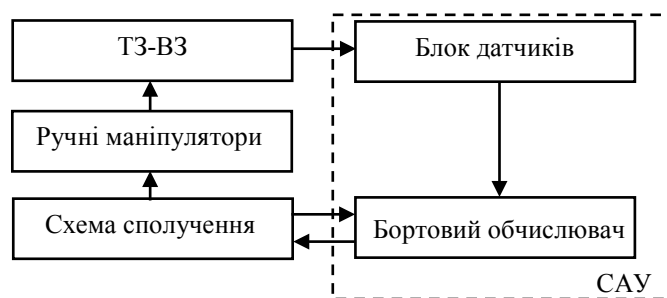


Рисунок 1 – Структура системи управління ТЗ-ВЗ

На систему покладається два основних завдання, а саме: приведення об'єкту ТЗ-ВЗ в бойову готовність та компенсація збурювальної дії ВЗ на транспортну базу.

Для вирішення цих завдань до складу САУ введено декілька контурів управління:

замкненого типу (горизонтування платформи на зупинці ТЗ);

розімкненого типу (відпрацювання сигналу управління вбудованого обчислювача з компенсації впливу ВЗ).

Синтез САУ замкненого типу широко представлено в науковій літературі і в даній роботі не розглядається.

Завдання іншого контуру – сформувати компенсаційний вплив на відкат при веденні вогню з урахуванням типу ВЗ, коливальних властивостей ТЗ, кута місця та кута за азимутом відносно поздовжньої осі ТЗ.

В роботі розглядається питання отримання передавальної функції розімкненого контуру САУ.

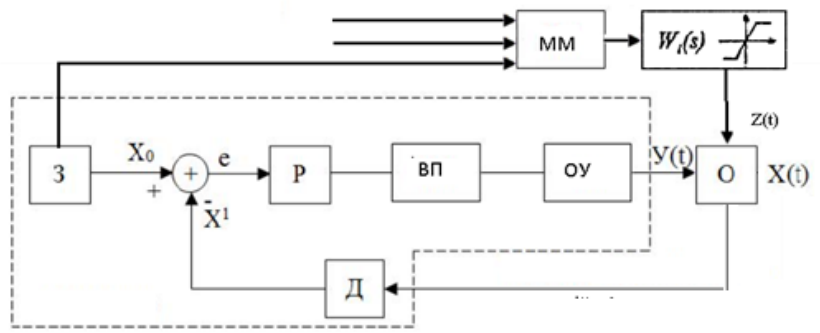


Рисунок 2 – Функціональна схема САУ

На рис.2 позначено: X_0 – сигнал інформації управління (в аналоговому або цифровому вигляді); Д – датчик; Р – регулятор [10]; ВП – виконавчий пристрій в замкненому контурі ОУ – орган управління; О – об’єкт регулювання [11]; $Y(t)$ – вплив управління; $Z(t)$ – сигнал збудження від пострілу; $X(t)$ – параметр регулювання; X_1 – сигнал на виході датчика; e – похибка; ММ – математична модель підресорної частини транспортної бази та ВЗ; $W_1(s)$ – передавальна функція виконавчого пристрою з обмеженням.

У розімкненій САУ вихід (положення поршня $x(t)$) не впливає на вхід (сигнал управління $u(t)$), тобто тривалість сигналу управління напряму визначає рух поршня.

Вважаємо, що час дії сигналу t лінійно пов’язаний з довжиною ходу $x(t)$, ($x(t)=K \cdot t$, де K – коефіцієнт пропорційності). Це вказує на інтегральний характер системи, яку плануємо створити.

Типова гідросистема включає:

джерело сигналу управління (спеціалізований обчислювач, контролер);

електромагнітний клапан управління дроселем;

гідроциліндр (виконавчий механізм).

Для синтезу САУ потрібно представити кожен елемент системи у вигляді передавальної функції $W(s)$. У системі автоматичного управління, загальна передавальна функція $W(s)$ є добутком передавальних функцій усіх її елементів (електромагнітний клапан, дросель (золотник), гідроциліндр) [12].

Джерело керуючого сигналу може бути представлено лінійною ланкою з певним коефіцієнтом підсилення.

Сигнал управління від спеціального обчислювача $u(t)$ подається без затримок та фільтрації. Отже, передавальна функція цієї ланки $W_1(s)$ має вид:

$$W_1(s) = K_u,$$

де K_u – коефіцієнт пропорційності.

Електромагнітний клапан забезпечує перетворення електричного сигналу певної тривалості t ($u(t)$) у витрату робочої рідини гідравлічної системи $Q(t)$. Зазвичай, через інерційність, електромагнітний клапан описується як система першого порядку:

$$Q(t) + \tau \dot{Q}(t) = K_v u(t),$$

де: K_v – коефіцієнт пропорційності електромагнітного клапана ($\text{м}^3/\text{сВ}$);

τ – стала часу клапана.

У S області передавальна функція електромагнітного клапана $W_2(s)$ має вид:

$$W_2(s) = \frac{Q(s)}{U(s)} = \frac{K_v}{1+\tau s}. \quad (1)$$

Гідроциліндр перетворює витрату рідини гідравлічної системи $Q(s)$ у положення поршня $x(t)$.

Для спрощеної моделі:

$$x(t) = \frac{Q(t)}{A},$$

У S області:

$$sX(s) = \frac{Q(s)}{A},$$

$$W_3(s) = \frac{X(s)}{Q(s)} = \frac{1}{As}.$$

Це інтегруюча ланка, що узгоджується з лінійною залежністю ходу поршня виконавчого пристрою від тривалості сигналу управління, адже інтеграл від постійного сигналу пропорційний часу.

Загальна передавальна функція $W(s)$ (добуток передавальних функцій елементів системи):

$$W(s) = W_1(s) \cdot W_2(s) \cdot W_3(s)$$

$$W(s) = K_u \cdot \frac{K_v}{1 + \tau s} \cdot \frac{1}{As}.$$

Після перетворення:

$$W(s) = \frac{K}{s(1+\tau s)}. \quad (2)$$

де: $K = \frac{K_u K_v}{A}$ – загальний коефіцієнт підсилення, s (у знаменнику) – інтегральна складова, $1 + \tau s$ – характеризує аперіодичну затримку електромагнітного клапана управління дроселем.

Вираз (2) передавальної функції характеризує ідеалі, які обумовлені масою рухомих частин (поршень, шток, навантаження), а також гідравлічною динамікою.

Якщо враховувати інерційні властивості системи, то рівняння руху поршня гідроциліндра має вид:

$$m\ddot{x}(t) + b\dot{x}(t) = F(t),$$

де m – маса рухомих частин, b – коефіцієнт в'язкого демпфування, $\ddot{x}$, $\dot{x}$ – прискорення та швидкість зміщення поршня.

Сила F , що діє на поршень з площею перетину A , пропорційна тиску P та спричиняє рух:

$$F(t) = P(t)A,$$

Рівняння руху в частотній області матиме вид:

$$ms^2X(s) + bsX(s) = P(s)A. \quad (3)$$

а сила:

$$F(s) = P(s)A.$$

Витрата рідини $Q(t)$ пов'язана зі швидкістю руху поршня $\dot{x}(t)$:

$$Q(t) = A\dot{x}(t) + \frac{V}{B}P(t),$$

де B – модуль пружності рідини (Па). Якщо вважати що рідина не стискається ($B \rightarrow \infty$), то:

$$Q(t) = A\dot{x}(t).$$

Зважаючи на (1), витрата рідини $Q(s)$ та сигнал управління $U(s)$ для клапана пов'язані виразом:

$$Q_k(s) = \frac{K_v}{1 + \tau s} U(s);$$

Для гідроциліндра:

$$Q_{ц}(s) = AsX(s), \quad (4)$$

Тиск $P(s)$ пов'язаний з витратами рідини $Q_{ц}(s)$ через гідравлічний опір R :

$$P(s) = Q_{ц}(s)R.$$

Тоді (3):

$$ms^2X(s) + bsX(s) = Q_{ц}(s)RA.$$

Підставимо значення витрат рідини в гідроциліндрі $Q_{ц}(s)$ (4):

$$ms^2X(s) + bsX(s) = RA(AsX(s)),$$

або:

$$ms^2X(s) + bsX(s) = RA^2sX(s). \quad (5)$$

Отримане рівняння (5) є рівнянням вільного руху.

Електромагнітний клапан управління дроселем та гідроциліндр є складовими однієї системи, а отже :

$$Q_k(s) = Q_{ц}(s)$$

$$AsX(s) = \frac{K_v}{1 + \tau s} U(s), \quad (6)$$

Припустимо $P(s)A = K_f Q_{ц}(s)$, де K_f – коефіцієнт перетворення витрат в силу. Тоді (3) матиме вид:

$$ms^2X(s) + bsX(s) = K_f Q_{ц}(s),$$

З врахуванням $Q_{ц}(s)$ (4):

$$ms^2X(s) + bsX(s) = K_f AsX(s).$$

Підставимо вираз $Q_k(s)$ з (6):

$$ms^2X(s) + bsX(s) = K_f \frac{K_v}{1 + \tau s} U(s).$$

Передавальна функція має вигляд:

$$X(s)(ms^2 + bs) = \frac{K_f K_v}{1 + \tau s} U(s),$$

$$W(s) = \frac{X(s)}{U(s)} = \frac{K_f K_v}{(ms^2 + bs)(1 + \tau s)}.$$

Після перетворень отримаємо:

$$W(s) = \frac{K_f K_v}{m\tau s^3 + (m + b\tau)s^2 + bs}.$$

Таким чином, отримано передавальну функцію розімкненого каналу САУ з врахуванням інерційності елементів. Це система третього порядку, де $m\tau s^3$ – інерція з врахуванням затримки клапана, $(m + b\tau)s^2$ – комбінація інерції та демпфування, bs – демпфування, τ – затримка клапана.

Висновки. У статті, на основі аналізу фізичних процесів і математичного моделювання основних компонент розімкненої системи автоматичного управління (джерела сигналу управління, електромагнітного клапана та гідроциліндра) отримано загальну передавальну функцію, яка враховує не лише динамічні характеристики кожного елемента, але й інерційні властивості цих елементів.

Особливу увагу приділено врахуванню реальних фізичних факторів, таких як: інерційність рухомих частин (поршня, штока, навантаження), демпфуючі ефекти та гідравлічна динаміка, що забезпечило уточнення моделі та підвищення її відповідності реальним умовам експлуатації. Отримана передавальна функція системи є важливим інструментом для подальшого аналізу стійкості, перехідних процесів та якості управління гідроприводами.

Запропонований підхід до моделювання має практичну цінність, оскільки може бути адаптований для проектування та оптимізації систем автоматичного управління в промислових і транспортних застосуваннях. Подальші дослідження можуть бути спрямовані на експериментальну верифікацію моделі та розробку алгоритмів адаптивного керування для підвищення ефективності роботи гідроприводів у змінних умовах.

ЛІТЕРАТУРА:

1. Wrata, G., Ranjan, P., Bhola, M., Mishra, S. K. and Das, J. (2019), "Position control and performance analysis of hydraulic system using two pumpcontrolling strategies". [Proceedings of the Institution of Mechanical Engineers], Part I: Journal of Systems and Control Engineering, 233(9), 1093-1105.
2. Minav, T., Laurila, L., and Pyrhönen, J. (2013), "Relative position control in an electro-hydraulic forklift". International Review of Automatic Control, 6(1), 54-61.
3. Буренніков Ю. А., Козлов Л. Г., Репінський С. В. Вибір параметрів системи керування гідроприводомз насосом змінної продуктивності на основі дослідження його стійкості. *Вісник Вінницького політехнічного інституту*. Вінниця: ВПІ, 2006. № 6. С. 211-217.
4. Міщук Д. О. Дослідження динамічної моделі гідравлічного циліндра об'ємного гідроприводу. *Гірничі, будівельні, дорожні та меліоративні машини: всеукр. зб. наук. праць*. Київ: КНУБА, 2016. Вип. 87. С. 74-81.
5. Буренніков Ю. А., Козлов Л. Г., Репінський С. В. Вибір параметрів системи керування гідроприводомз насосом змінної продуктивності на основі дослідження його стійкості. *Вісник Вінницького політехнічного інституту*. Вінниця: ВПІ, 2006. № 6. С. 211-217.
6. Крутіков Г. А., Стрижак М. Г. Синтез параметрів електрогідравлічного слідкуючого привода виходячи з заданої точності позиціонування робочого органа, швидкодії і характеру перехідного

процесу. *Вісник Національного технічного університету "ХПІ"*. Харків: ХПІ, 2022. №2. С. 35-40. DOI 10.20998/2079-0775.2022.2.04

7. Маловичко В. К., Брунеткін О. І. Дослідження автоматичної системи регулювання рівня води в групі підігрівачів високого тиску. *Інформатика, обчислювальна техніка та автоматизація*. К.: ТНУ імені В.І. Вернадського, 2021. №3 Том 32(71) С. 117-122.

DOI 10.32838/2663-5941/2021.3/19

8. Голубенко О. Л., Романченко О. В., Соколов В. І., Степанова О. Г. Методика проектного розрахунку автоматичного електрогідравлічного приводу обертального руху та об'ємного регулювання. *Вісник східноукраїнського національного університету*. К.: ВСУ імені Володимира Даля, 2022. №2(272) С. 15-22. DOI 10.33216/1998-7927-2022-272-2-15-22

9. Bezuhlyi, V., Oliynyk, V., Romanenko I., Zhuk, O., Kuzavkov, V., Borysov, O., Korobchenko, S., Ostapchuk, E., Davydenko, T., and Shyshatskyi, A. (2021). "Development of object state estimation method in intelligent decision support systems". *Eastern-European Journal of Enterprise Technologies*, 5(3 (113), 54-64. DOI 10.15587/1729-4061.2021.239854

10. Гостев В.І., Кузавков В.В. Параметричний синтез цифрових псевдолінійних коригувальних пристроїв Том 29, Випуски 2-3, 1997, С. 133-136 DOI 10.1615/JAutomatInfScien.v29.i2-3.170

11. Кузавков, В., Поляк, І. Аналіз транспортної бази для встановлення стабілізованої платформи нетипової артилерійської системи. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво*, 2023, (50), С. 15-20. DOI 10.36910/6775-2524-0560-2023-50-02

12. Qiu, Hanyu, and Qi, Su. (2021), "Simulation Research of Hydraulic Stepper Drive Technology Based on High Speed On/Off Valves and Miniature Plunger Cylinders". *Micromachines* 12.4, 438. DOI 10.3390/mi12040438.

REFERENCES:

1. Wrata, G., Ranjan, P., Bhola, M., Mishra, S. K. and Das, J. (2019), "Position control and performance analysis of hydraulic system using two pumpcontrolling strategies". [Proceedings of the Institution of Mechanical Engineers], Part I: Journal of Systems and Control Engineering, 233(9), 1093-1105.

2. Minav, T., Laurila, L., and Pyrhönen, J. (2013), "Relative position control in an electro-hydraulic forklift". *International Review of Automatic Control*, 6(1), 54-61.

3. Buriennikov Yu. A., Kozlov L. H., Repinskyi S. V. Vybir parametriv systemy keruvannia hidropriyodomz nasosom zminnoi produktyvnosti na osnovi doslidzhennia yoho stiikosti. *Visnyk Vinnytskoho politekhnichnoho instytutu*. Vinnytsia: VPI, 2006. № 6. S. 211-217.

4. Mishchuk D. O. Doslidzhennia dynamichnoi modeli hidravlichnoho tsylindra obiemnoho hidropriyodu. *Hirnychi, budivelni, dorozhni ta melioratyvni mashyny: vseukr. zb. nauk. prats*. Kyiv: KNUBA, 2016. Vyp. 87. S. 74-81.

5. Buriennikov Yu. A., Kozlov L. H., Repinskyi S. V. Vybir parametriv systemy keruvannia hidropriyodomz nasosom zminnoi produktyvnosti na osnovi doslidzhennia yoho stiikosti. *Visnyk Vinnytskoho politekhnichnoho instytutu*. Vinnytsia: VPI, 2006. № 6. S. 211-217.

6. Krutikov H. A., Stryzhak M. H. Syntez parametriv elektrohivavlichnoho slidkuiuchoho pryvoda vykhodiachy z zadanoi tochnosti pozytsiiuvannia robochoho orhana, shvydkodii i kharakteru perekhidnoho protsesu. *Visnyk Natsionalnoho tekhnichnoho universytetu "KhPI"*. Kharkiv: KhPI, 2022. №2. S. 35-40. DOI 10.20998/2079-0775.2022.2.04

7. Malovychko V. K., Brunetkin O. I. Doslidzhennia avtomatychnoi systemy rehuliuвання рівня води в групі підігрівачів високого тиску. *Інформатика, обчислювальна техніка та автоматизація*. К.: ТНУ імені В.І. Вернадського, 2021. №3 Том 32(71) С. 117-122. DOI 10.32838/2663-5941/2021.3/19

8. Holubenko O. L., Romanchenko O. V., Sokolov V. I., Stepanova O. H. Metodyka proektnoho rozrakhunku avtomatychnoho elektrohivavlichnoho pryvodu obertalnoho rukhu ta obiemnoho rehuliuвання. *Visnyk skhidnoukrainskoho natsionalnoho universytetu*. К.: VSNU імені Volodymyra Dalia, 2022. №2(272) С. 15-22. DOI 10.33216/1998-7927-2022-272-2-15-22

9. Bezuhlyi, V., Oliynyk, V., Romanenko I., Zhuk, O., Kuzavkov, V., Borysov, O., Korobchenko, S., Ostapchuk, E., Davydenko, T., and Shyshatskyi, A. (2021). "Development of object state estimation method in intelligent decision support systems". *Eastern-European Journal of Enterprise Technologies*, 5(3 (113), 54-64. DOI 10.15587/1729-4061.2021.239854

10. Hostiev V.I., Kuzavkov V.V. Parametrychnyi syntez tsyfrovyykh psevdoliniinykh koryhuvalnykh prystroiv Tom 29, Vypusky 2-3, 1997, C. 133-136. DOI 10.1615/JAutomatInfScien.v29.i2-3.170
11. Kuzavkov, V., Poliak, I. Analiz transportnoi bazy dlia vstanovlennia stabilizovanoi platformy netypovoi artyleriiskoi systemy. Kompiuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo, 2023, (50), C. 15-20. DOI 10.36910/6775-2524-0560-2023-50-02
12. Qiu, Hanyu, and Qi, Su. (2021), "Simulation Research of Hydraulic Stepper Drive Technology Based on High Speed On/Off Valves and Miniature Plunger Cylinders". Micromachines 12.4, 438. DOI 10.3390/mi12040438.

**Dr. Tech. Sci., prof. Minochkin A.I., Dr. Tech. Sci., prof. Kuzavkov V.V.,
Ph.d.. Romanenko M.M.**

TRANSFER FUNCTION OF AN OPEN-CIRCUIT AUTOMATIC CONTROL SYSTEM WITH HYDRAULIC DRIVE

The article derives the transfer function of the automatic control system with hydraulic cylinders as an actuator. The need to obtain a model is associated with the synthesis of one of the system channels.

The general automatic control system contains several control channels. The system is built for a specific object. This is a unified stabilization platform for an atypical firearm on a highly mobile transport base. One of the tasks of the automatic control system is to compensate for the impact of the use of a firearm. Control occurs according to the mathematical model of the firearm - vehicle object. The synthesis of feedback channels present in the system is not considered in the work. The main attention is paid to modeling processes in a channel without feedback. This option for constructing (the automatic control system channel) and choosing an actuator is due to the type of external influence on the control object (a short-term high-intensity pulse).

Mathematical modeling of the main components of an open system: a control signal source, a solenoid valve and a hydraulic cylinder was carried out taking into account the processes occurring in the elements of the system.

Based on the transfer functions of individual components, the general transfer function of the system (control channel) was determined. In addition, inertial characteristics arising from the mass of moving parts (piston, rod, load), damping factors and hydraulic dynamics were taken into account. As a result, a refined mathematical model of an automatic control system with a hydraulic drive was obtained, which reflects the dynamic properties of the system taking into account real physical processes.

The proposed approach can be used for further analysis of the stability and quality of control of hydraulic drives in industrial and transport applications.

Keywords: control channel, automatic control system, transfer function, feedback, actuator, hydraulic system, fire vehicle, transport base.

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ РОЗРОБЛЕНИХ АЛГОРИТМІВ ТА МОДЕЛЕЙ ЗАХИСТУ В МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ

У статті розглянуто питання моделювання трафіку та оцінювання ефективності алгоритмів захисту інформації в мережах IoT. Проведено імітаційне моделювання сценаріїв з різними моделями трафіку, аналіз роботи захисних алгоритмів для виявлення атак, створено рекомендації до практичного застосування в інфраструктурі IoT з урахуванням специфіки 5G мереж інтернет речей.

Під час дослідження було проаналізовано специфіку структури мереж Інтернету речей, визначено ключові метрики трафіку та побудовано математичну модель на основі класичної моделі Пуассона, а також її розширень ММРР та ВМАР для адекватного відображення змінної та кластерної структури трафіку в мережах Інтернету речей. Кластеризацію виконували за допомогою алгоритму k-середніх для профілювання нормальної поведінки вузлів, що дозволило виявляти аномалії в режимі реального часу. Було запропоновано формальну модель оцінки ризиків, яка враховує відхилення поточних метрик від типового кластера та зміни інтенсивності. Розроблено адаптивний механізм реагування на інциденти з пороговими значеннями, що визначають рівень втручання від обмеження активності до повного блокування пристрою. Для верифікації було змодельовано сценарії DDoS, підміни пристроїв та прихованої атаки. Ефективність алгоритму виявлення оцінювали за допомогою метрик точності, повноти, F1-оцінки та часу відгуку.

Результати показали, що запропонована методологія забезпечує високу точність виявлення аномалій (F1-оцінка = 92,5%) з часом відгуку до 80 мс, що робить її придатною для використання в реальних системах Інтернету речей. Запропонований підхід дозволяє підвищити надійність та безпеку мережі без значного збільшення обчислювальних витрат. Отримані результати підтверджують доцільність впровадження інтелектуальних систем моніторингу на основі кластеризації та моделей ризиків в інфраструктурі 5G-IoT.

Ключові слова: моделювання трафіку, кібербезпека, алгоритми захисту, 5G, IDS, аномалії.

Постановка проблеми. Інтернет речей (Internet of Things, IoT) стрімко трансформує сучасні інформаційні технології, забезпечуючи зв'язок між фізичними об'єктами та цифровим середовищем. Важко уявити сучасне місто чи будинок, чи бізнес, в якому б не використовувались різноманітні системи спостереження, контролю доступу чи фіксації стану, які належать системам IoT. У 2025 році очікується, що кількість таких пристроїв перевищить 30 мільярдів, що ставить перед науковою спільнотою низку викликів, зокрема, пов'язаних з забезпеченням їх безпеки, ефективним управлінням трафіком, масштабованістю мереж та підтримкою QoS.

Особливу роль відіграє взаємодія IoT з мережею 5G, яка забезпечує високу швидкість передачі даних, малу затримку та масову підтримку пристроїв. Проте, водночас, виникає потреба в адаптації механізмів захисту інформації до нових умов функціонування, а саме: обмежених обчислювальних ресурсів пристроїв, змінності трафіку, підвищеного ризику атак з боку злоумисників та широкого використання бездротових протоколів зв'язку.

Аналіз останніх досліджень та публікацій. Наразі існує багато підходів до організації захисту мереж IoT – від класичних методів шифрування до систем виявлення аномалій, заснованих на методах машинного навчання. Проте, більшість з них, не враховують специфіку трафіку, обмеження обчислювальних ресурсів та реальні сценарії функціонування мереж.

У цьому контексті особливої ваги набуває розробка математичних моделей, які здатні точно відображати поведінку IoT-мереж і трафіку, а також методології оцінки ефективності алгоритмів захисту в таких умовах.

Постановка завдання. Таким чином метою статті є дослідження ефективності існуючих і розроблених алгоритмів захисту IoT-мереж шляхом побудови імітаційної моделі мережі, проведення експериментів та формалізації отриманих результатів у вигляді методології.

Виклад основного матеріалу. Моделювання процесів у мережах Інтернету речей (IoT) є ключовим інструментом для аналізу їх функціонування, виявлення потенційних загроз та тестування алгоритмів безпеки. У даному дослідженні запропонована структурована методологія моделювання, яка включає етапи побудови топології, опису трафіку, моделювання подій, та аналізу показників ефективності.

Основними цілями моделювання є аналіз поведінки мережі під навантаженням, оцінка ефективності алгоритмів виявлення атак, вивчення взаємодії вузлів у різних режимах трафіку, перевірка механізмів QoS та стійкості до атак.

В розрізі розвитку IoT, вимогами до моделі є масштабованість (будемо розглядати до тисяч пристроїв), підтримка різних класів пристроїв (сенсори, актуатори, шлюзи), можливість впровадження атак (spoofing, DDoS, MitM), підтримка моделей трафіку з часовою варіативністю (MMPP, BMAP).

Щодо архітектури моделі мережі, то вона має три рівні абстракції, а саме рівень пристроїв (вузли з обмеженими обчислювальними ресурсами, що генерують трафік), рівень комунікацій (протоколи з'єднання MQTT, CoAP, 6LoWPAN, типи каналів LoRa, Wi-Fi, NB-IoT), рівень обробки даних (локальні шлюзи та хмарна інфраструктура, які аналізують і маршрутизують трафік).

Для реалізації моделі IoT використовуються інструменти, які забезпечують точне відтворення процесів та мережесхем сценаріїв. У рамках роботи можливі такі середовища:

1) OMNeT++ з модулем INET – моделювання протоколів, маршрутизації, пакетного трафіку.

2) NS-3 – для більш низькорівневого моделювання радіоканалів та стеків зв'язку.

3) SimPy + Python – створення гнучких симуляцій з кастомною логікою.

Класифікація трафіку, що моделюється як набір випадкових процесів з урахуванням типу пристрою поділяється на періодичний (сенсори температури, освітлення), подієвий (сигналізація, розпізнавання руху), та агрегований (вузли збору даних).

Кожен тип моделюється окремо з параметрами $\lambda(t), \sigma^2, \Delta t$ тощо. Наприклад, для подієвих вузлів застосовуються марковські процеси зі змінною інтенсивністю:

$$P(N(t) = k) = \frac{(\lambda t)^k}{k!} e^{-\lambda t}, \lambda = \lambda_i, X(t) = i \quad (1)$$

де $X(t)$ - марковський стан активності вузла.

Для дослідження ефективності алгоритмів та моделей у мережах Інтернету речей був розроблений поетапний алгоритм моделювання, що дозволяє відтворити реалістичну поведінку IoT-мережі та врахувати особливості трафіку й можливі загрози. Запропоновано та впроваджено наступні ключові кроки:

1. Генерація топології мережі. Модель мережі формується у вигляді орієнтованого або неорієнтованого графа $G=(V,E)$, де множина вершин V відповідає IoT-пристроєм, шлюзам, серверам, а множина ребер E – зв'язкам між ними, вузли мають різний тип (сенсори, актуатори, шлюзи), зв'язки можуть бути бездротовими або провідними, із визначеною пропускну здатністю і затримкою. Ця структура задається як вхідний параметр або генерується випадковим чином за правилами топології, що відтворюють реальні IoT-мережі.

2. Призначення типу трафіку кожному вузлу. Кожен вузол отримує характеристику трафіку на основі класу пристрою: періодичний сенсорний трафік (з фіксованою або змінною частотою), подієвий трафік, що активується у відповідь на події.

3. Агрегований трафік з передачею пакетів групами, типи трафіку визначаються із застосуванням моделей Пуассона, ММРР, ВМАР. Цей крок є важливою складовою моделювання поведінки мережі, що дозволяє точніше симулювати навантаження.

4. Встановлення подій у мережі. Для дослідження стійкості мережі вводяться такі події: ініціація атак (наприклад, підміна вузла, DoS-атаки), моделювання збоїв обладнання або каналів, пікові навантаження, що імітують пікові періоди роботи. Події розподіляються у часі й просторі, що дає можливість оцінити динаміку роботи захисних механізмів у різних умовах.

5. Запуск симуляції на часовому інтервалі $[0, T]$. Симуляція виконується протягом заданого проміжку часу, де відстежуються: передача пакетів між вузлами, зміни в інтенсивності трафіку відповідно до моделей.

6. Виявлення подій і реагування алгоритмів захисту. Використовується дискретне або подієве моделювання, що дозволяє зафіксувати ключові параметри та часові відрізки.

7. Запис та агрегація результатів. Після завершення симуляції збираються та аналізуються такі показники: затримки передачі даних по мережі, навантаження на канали і вузли, втрати пакетів.

8. Коефіцієнти виявлення атак і хибних спрацювань. Ці дані формують основу для подальшого аналізу ефективності та вдосконалення алгоритмів захисту.

Метрики оцінювання:

1. Середня затримка (delay)

$$D = \frac{1}{N} \sum_{i=1}^N (t_i^{recv} - t_i^{send}) \quad (2)$$

2. Пропускна здатність (throughput)

$$T = \frac{\sum_{i=1}^N s_i}{T_{sim}} \quad (3)$$

3. Відсоток виявлених атак (detection rate)

$$DR = \frac{TP}{TP + FN} \quad (4)$$

4. Помилкові спрацювання (false positives)

$$FP_{rate} = \frac{FP}{FP + TN} \quad (5)$$

IoT-трафік характеризується високим ступенем гетерогенності, залежністю від типу пристрою, режиму роботи, частоти генерації даних та типу подій. Для ефективного моделювання трафіку мереж IoT в цій роботі було використано кілька класичних та сучасних моделей трафіку, а саме:

1) Модель Пуассона – це математична модель, яка описує випадковий процес, де кількість подій $N(t)$, що відбулися за проміжок часу, підпорядковуються розподілу Пуассона.

Наведений нижче код реалізує генерацію синтетичного трафіку відповідно до Пуассонівської моделі, яка широко застосовується в телекомунікаційних системах та зокрема в IoT-середовищах для опису регулярного, періодичного трафіку з постійною середньою інтенсивністю подій. У цьому прикладі симуляція здійснюється у часовому інтервалі

$T = 100c$ із дискретним кроком $\Delta t = 0,1c$. Інтенсивність надходження подій задана як $\lambda = 5$ подій за секунду. Отже, очікувана кількість подій на кожному інтервалі Δt становить $\lambda \times \Delta t = 0,5$. Для кожного кроку часу випадкова кількість подій генерується з використанням розподілу Пуассона. Код також містить побудову графіка, який демонструє характер надходження подій у часі: на осі абсцис відкладається час, а на осі ординат – кількість подій (пакетів), згенерованих протягом відповідного інтервалу. Застосування стилю «steps-post» надає графіку дискретного, "сходиноквого" вигляду, що краще відповідає природі-процесу Пуассона, як марковського випадкового процесу з незалежними інтервалами між подіями.

```
import numpy as np
import matplotlib.pyplot as plt

T = 100 # тривалість симуляції (сек)
dt = 0.1 # часовий крок
time = np.arange(0, T, dt)
lambda_rate = 5 # інтенсивність подій (подій/сек)
packets = np.random.poisson(lambda_rate * dt, len(time))
plt.plot(time, packets, drawstyle='steps-post')
plt.title("Пуассонівський трафік")
plt.xlabel("Час (с)")
plt.ylabel("Кількість подій")
plt.grid(True)
plt.show()
```

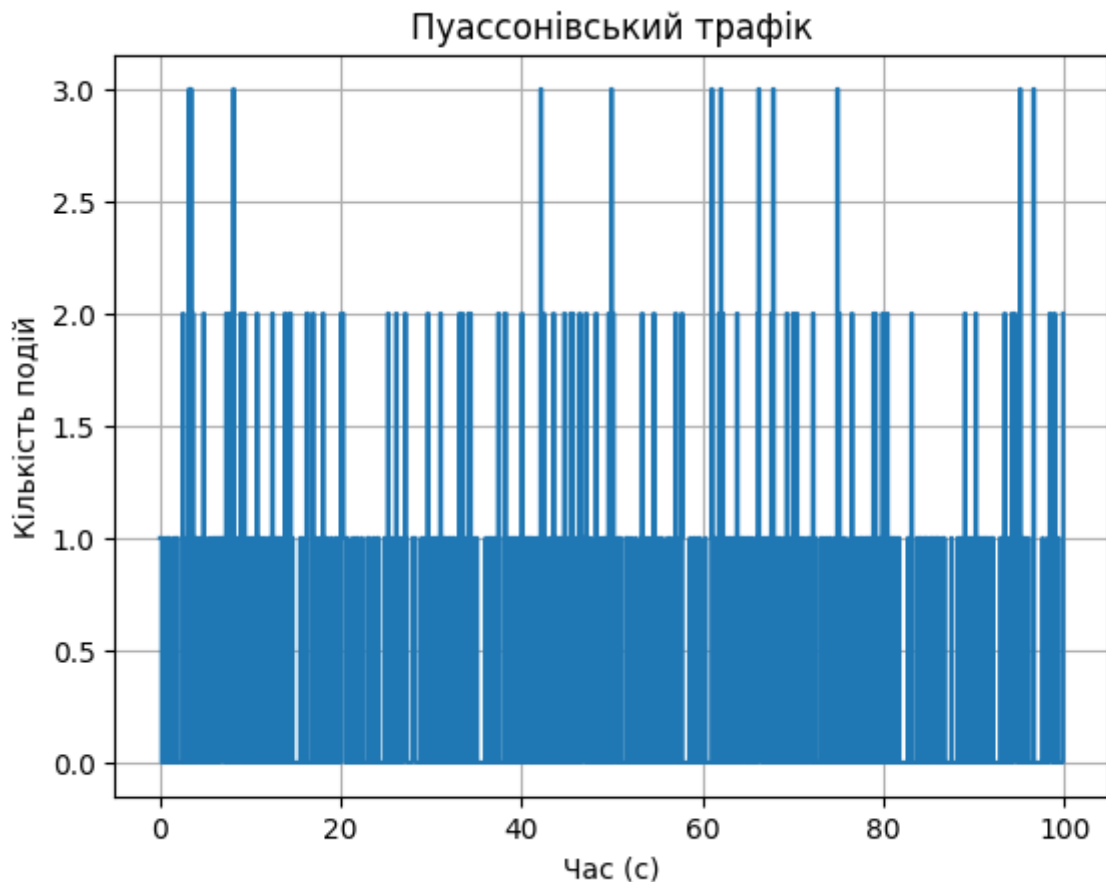


Рисунок 1 - Результат симуляції трафіку згідно з Пуассонівською моделлю. Графік

відображає кількість згенерованих подій у часі в межах дискретної симуляції. Розроблено авторами

2) Модель MMPP (Markov Modulated Poisson Process) – це стохастичний процес, в якому інтенсивність надходження подій (трафіку) змінюється у часі залежно від стану прихованого марковського процесу.

$$\lambda(t) = \sum_{i=1}^n \lambda_i \times I_{X(t)=i} \quad (6)$$

де λ_i – інтенсивність надходження подій (пакетів) у стані i , $X(t)$ – неперервний марковський процес, що визначає поточний стан системи у часі, $I_{X(t)=i}$ – індикатор функції: дорівнює 1, якщо система в стані i і 0 – якщо в іншому стані.

Програмна реалізація ілюструє симуляцію процесу генерації трафіку в мережах IoT на основі марковського процесу з модуляцією інтенсивності.

```
import numpy as np
import matplotlib.pyplot as plt

T = 100
dt = 0.1
time = np.arange(0, T, dt)
lambda_low = 1
lambda_high = 10
Q = np.array([[0.1, 0.1],
              [0.05, -0.05]])
state = 0
states = []
arrivals = []
for t in time:
    states.append(state)
    lam = lambda_low if state == 0 else lambda_high
    arrivals.append(np.random.poisson(lam * dt))
    if state == 0 and np.random.rand() < Q[0, 1] * dt:
        state = 1
    elif state == 1 and np.random.rand() < Q[1, 0] * dt:
        state = 0
plt.figure(figsize=(10, 5))
plt.subplot(2, 1, 1)
plt.plot(time, states, drawstyle='steps-post')
plt.title("Стан системи (MMPP)")
plt.ylabel("Стан")
plt.subplot(2, 1, 2)
plt.plot(time, arrivals, drawstyle='steps-post')
plt.title("MMPP: надходження пакетів у часі")
plt.xlabel("Час (с)")
plt.ylabel("Кількість подій")
plt.tight_layout()
plt.show()
```

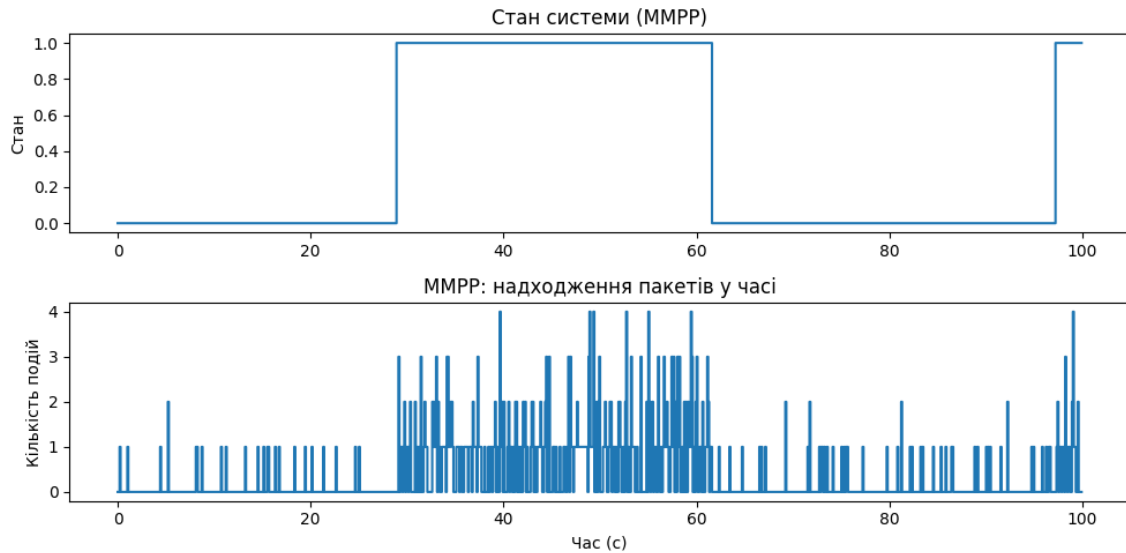


Рисунок 2 - Результат симуляції трафіку згідно з моделлю MMPP.
Розроблено авторами

3) BMAP (Batch Markovian Arrival Process) – це марковський процес пакетних надходжень, що дозволяє моделювати моменти надходження подій та їх кількість.

$$D = \sum_{k=0}^{\infty} D_k \quad (7)$$

де D_k – набір матриць, в якому кожна окрема матриця відображає імовірності переходу між станами з генерацією k пакетів, D_0 – імовірність переходу без генерації пакетів, D_1 – перехід з генерацією 1 пакету і т.д.

В програмному коді реалізовано імітаційну модель пакетного трафіку в мережах IoT.

```
import numpy as np
import matplotlib.pyplot as plt
T = 100
dt = 0.1
time = np.arange(0, T, dt)
# Пакети приходять "пачками" по 3–10 штук залежно від стану
states = [0, 1] # стан 0 - мала група, стан 1 - велика група
packet_sizes = {0: (3, 5), 1: (6, 10)} # інтервали кількості пакетів
Q = np.array([[0.05, 0.05],
[0.02, -0.02]])
state = 0
arrivals = []
for t in time:
    size_range = packet_sizes[state]
    packets = np.random.randint(size_range[0], size_range[1]+1)
    arrivals.append(packets)
    if state == 0 and np.random.rand() < Q[0, 1] * dt:
        state = 1
    elif state == 1 and np.random.rand() < Q[1, 0] * dt:
        state = 0
plt.plot(time, arrivals, drawstyle='steps-post')
plt.title("BMAP: пакетна передача даних")
```

```
plt.xlabel("Час (с)")
plt.ylabel("Кількість пакетів")
plt.grid(True)
plt.show()
```

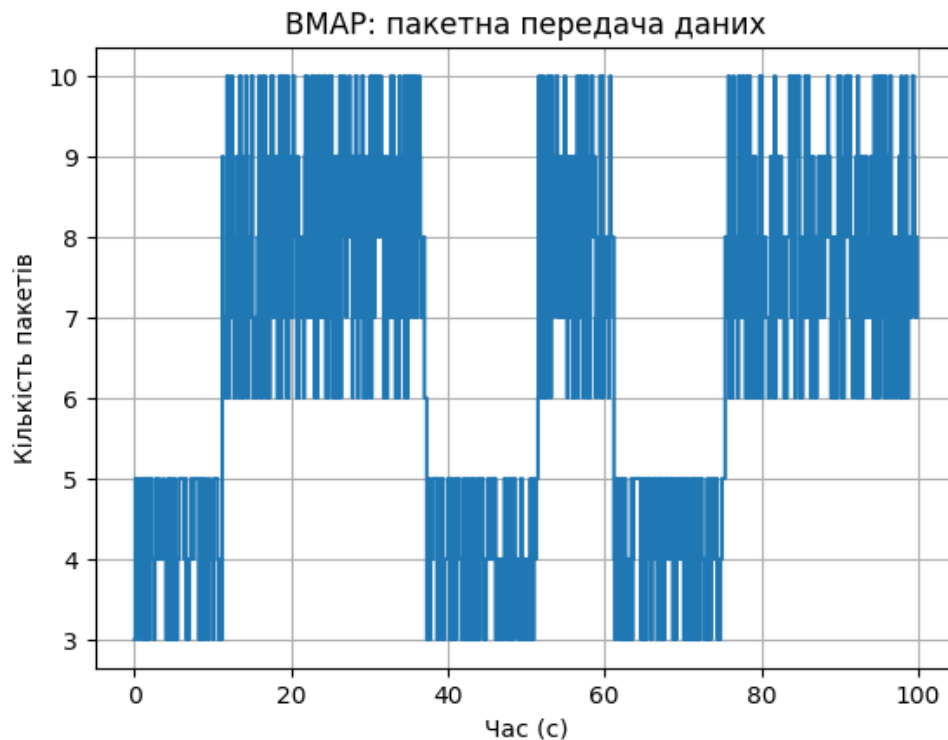


Рисунок 3. - Результат симуляції трафіку згідно з моделлю ВМАР.
Розроблено авторами

Таблиця 1

Порівняльна характеристика моделей трафіку для мереж IoT

Модель	Тип даних	Гнучкість	Складність	Підтримка подієвості
Пуассона	періодичний	низька	низька	ні
ММРР	подієвий/реактив	середня	середня	так
ВМАР	агрегований	висока	висока	частково

Тепер розглянемо як захистити IoT мережу та виявити відхилення чи аномалії. Виявлення аномалій базується на аналізі відхилень від еталонної поведінки трафіку. Нехай $X = \{x_1, x_2, \dots, x_n\}$ набір ознак трафіку, наприклад, середня інтенсивність пакету, дисперсія та частота надходження пакетів.

Визначимо відстань $\rho(x_i, \mu_i)$ між точкою x_i та центром кластера μ_i . Якщо $\rho(x_i, \mu_i) > \tau$ (порогове значення), то точка вважається аномалією.

Для моніторингу нормального стану мережі та наявності різного роду відхилень, починаючи від виходу з ладу одного з датчиків та закінчуючи DDoS атаками зручно використовувати алгоритм кластеризації k-means. Мета алгоритму — мінімізувати суму квадратів відстаней до центрів кластерів:

$$J = \sum_{j=1}^k \sum_{x_i \in C_j} \|x_i - \mu_j\|^2$$

де k - кількість кластерів, C_j - кластер j , μ_j - центр кластера j .

Отже, кластеризація за допомогою k-means може бути використана як базовий механізм виявлення аномалій. Алгоритм легко масштабується, не потребує попереднього маркування даних і може працювати в онлайн-режимі при періодичному оновленні кластерів.

Проте захист інфраструктури Інтернету речей в умовах високої варіативності трафіку та обмежених обчислювальних ресурсів вимагає впровадження багаторівневої адаптивної системи. Нижче запропонована методологія базується на комбінуванні поведінкового аналізу, кластеризації та математичного моделювання трафіку.

Спочатку розглянемо принципи побудови адаптивного захисту. Поведінка IoT-пристроїв оцінюється з урахуванням моделі MMPP або BMAP, що дозволяє виявити сплески активності, відхилення від профілю, захист реалізується на трьох рівнях: сенсорному (рівень пристроїв), мережевому (шлюзи, маршрутизатори) та хмарному (аналітика та верифікація). А також інтеграція засобів аналізу трафіку (використання IDS/IPS-систем із машинним навчанням на основі кластеризації) та автономна обробка edge computing (мінімізація часу реакції на загрозу за рахунок обробки на шлюзовому рівні).

Наступним етапом розглянемо архітектуру захисної моделі. Модель включає три рівні з відповідною функціональністю, а саме:

1. Пристрої IoT Edge (криптографічна аутентифікація (наприклад, ECC), контроль MAC-адрес та унікальних ідентифікаторів та обмежена обробка поведінкових шаблонів).
2. Шлюзи/Прикордонні вузли (профілювання трафіку за допомогою кластеризації (k-means, DBSCAN), аналіз часових серій інтенсивності на основі моделі MMPP, а також локальне виявлення аномалій:

$$a_i = \begin{cases} 1, \text{ якщо } \|x_i - \mu_j\|^2 > \tau \\ 0, \text{ якщо інакше} \end{cases}$$

3. Хмарна платформа (централізована база профілів пристроїв, кореляція подій між кількома доменами та довгострокове машинне навчання).

Відповідно до ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT) при розробці захисту мережі ми повинні розглядати також і оцінки ризиків. Рівень ризику оцінюється як функція двох чинників:

$$R(x_i) = \alpha \times \|x_i - \mu_j\|^2 + \beta \times |\lambda_i - \bar{\lambda}_j|$$

де x_i - вектор поточних метрик трафіку, μ_j - центр профільного кластера, λ_i - інтенсивність, $\bar{\lambda}_j$ - середня інтенсивність для кластера, α, β - вагові коефіцієнти ризику (налаштовуються політикою безпеки).

Згідно з отриманими даними, наступним етапом ми розробляємо алгоритм реагування на інциденти, а саме:

1. Профілювання: кластеризація трафіку (offline-етап). За допомогою алгоритму кластеризації (наприклад, k-means) формується набір еталонних кластерів трафіку, що відповідають нормальній роботі пристроїв.
2. Моніторинг (online-етап). На цьому етапі в реальному часі постійно фіксується нова інформація про трафік, що надходить від пристроїв, кожна нова порція даних описується у вигляді вектора ознак.

3. Оцінка ризику: обчислення $R(x_i)$, що обчислюється для кожного нового вектору.
4. Реакція на аномалію:

якщо: $R(x_i) > \theta$ підозра на аномалію, система обмежує активність пристрою (блокує окремі типи трафіку, зменшує швидкість тощо);

якщо : $R(x_i) > 2\theta$ критичне відхилення від норми, можлива атака чи вторгнення в мережу, відбувається повне блокування пристрою, а також здійснюється надсилання оповіщення адміністратору;

якщо: $R(x_i) < \theta$ відхилення незначне, пристрій працює в нормальному режимі, дія відсутня.

Щоб підтвердити практичну ефективність розробленої методології виявлення та реагування на загрози в IoT-мережах, було проведено моделювання типових сценаріїв атак у контрольованому середовищі. Це дозволило протестувати алгоритм в умовах, наближених до реальних, але з відомими параметрами, що важливо для верифікації.

Було змодельовано три ключові типи загроз, що характерні для Інтернету речей, а саме підміна пристрою (spoofing), інтенсивну DDoS-атаку та скритну атаку (evasion).

Для об'єктивного аналізу якості виявлення атак були використані класичні метрики машинного навчання:

1. Precision, що показує, яка частка спрацьовувань системи дійсно була правильною (тобто скільки з усіх виявлених інцидентів реально були загрозами). Отримано: 93.7%, що є дуже високим показником, тобто система майже не помиляється, коли сигналізує про загрозу.
2. Recall, що відображає, яка частка всіх загроз була виявлена системою. Отримано: 91.4%, що означає, що система виявила більшість атак, лише деякі залишились непоміченими.
3. F1-score – гармонійне середнє між precision і recall, що дає збалансовану оцінку ефективності системи. Отримано: 92.5%, що підтверджує високу загальну якість класифікації.
4. Час реакції до 80 мс – означає, що система миттєво (у межах сотень мілісекунд) реагує на загрозу.

Таблиця 2

Отримані результати

Метрика	Значення
Precision	93.7%
Recall	91.4%
F1-score	92.5%

Ці результати підтверджують придатність методології до впровадження у реальних системах з обмеженими ресурсами та змінною топологією мережі IoT.

Висновки. У цій роботі було виконано комплексне дослідження, спрямоване на створення методологічної та математичної основи для побудови ефективної системи захисту мереж Інтернету речей в умовах використання технологій 5G. В роботі проведено огляд особливостей трафіку в IoT-мережах, встановлено, що класичні моделі типу Пуассона не забезпечують достатньої точності при відтворенні реактивного та подієвого трафіку. Розглянуто та здійснено порівняльну характеристику математичних моделей трафіку, серед яких найбільш ефективними виявилися MMPP та ВМАР процеси, здатні відтворювати реалістичні сценарії функціонування IoT-пристроїв, включаючи періоди активності, сплесків передачі інформації та пакетну передачу даних.

На основі аналізу характеристик трафіку було запропоновано метод виявлення аномалій, що ґрунтується на кластеризації профілів трафіку та оцінці відхилень від центрів кластерів. Формалізовано підхід до оцінювання ризику вторгнення за допомогою квадратичної метрики та зміни інтенсивності трафіку.

Запропоновано багаторівневу архітектуру захисту, яка охоплює рівень сенсорів, шлюзів та хмарної інфраструктури. Визначено відповідну функціональність кожного рівня, включаючи локальне виявлення аномалій, криптографічний захист, edge-аналітику та централізовану обробку подій. Методика адаптивного реагування на інциденти включає обчислення ризику, визначення порогових значень та автоматизоване прийняття рішень щодо обмеження чи блокування підозрілої активності. Це дозволяє значно скоротити час реагування на атаки, знизити ймовірність компрометації та підвищити надійність мережі IoT. Проведено імітаційне моделювання роботи системи захисту, результати якого підтвердили високу точність виявлення атак типу DDoS, spoofing та прихованих вторгнень. Досягнута точність виявлення понад 93% та середній час реакції до 80 мс свідчать про ефективність запропонованих підходів навіть за умови обмежених обчислювальних ресурсів.

Отже, результати цього дослідження дозволяють зробити висновок про доцільність впровадження адаптивної, багаторівневої системи захисту в IoT-мережах з використанням сучасних моделей трафіку та алгоритмів аналізу аномалій. Подальші дослідження можуть бути зосереджені на апаратній реалізації моделей, розробці легковагових IDS для edge-пристроїв та інтеграції з 5G-мережами шляхом використання slicing-політик та QoS-контролю.

ЛІТЕРАТУРА:

1. Андрійчук М. Моделювання трафіку в мережах Інтернету речей / М. Андрійчук // *Радіoeлектроніка, інформатика, управління*. – 2020. – № 2. – С. 15 – 23.
2. Ковальчук В. Особливості використання протоколу MQTT в IoT / В. Ковальчук, І. Іванова // *Наукові праці ОНАЗ ім. О. С. Попова*. – 2019. – № 4. – С. 56 – 62.
3. Лапко А. Імітаційне моделювання захисту мережі IoT / А. Лапко, С. Притула // *Вісник НТУУ «КПІ»*. Серія: Інформатика та обчислювальна техніка. – 2021. – № 75. – С. 44 – 50.
4. Гриценко В. Підходи до побудови IDS для IoT / В. Гриценко, М. Соловей // *Системи обробки інформації*. – 2022. – № 3(172). – С. 27–34.
5. Мельник О. Використання марковських процесів для опису трафіку IoT / О. Мельник // *Математичне моделювання та обчислювальні методи*. – 2020. – Т. 2, № 1. – С. 91 – 99.
6. Chen S. A survey on industrial Internet of Things security architecture / S. Chen, H. Xu, D. Liu et al. // *Future Internet*. – 2020. – Vol. 12(1). – P. 1 – 18.
7. Alrawais A. Fog computing for the Internet of Things: Security and privacy issues / A. Alrawais, A. Alhothaily, C. Hu, X. Cheng // *IEEE Internet Computing*. – 2017. – Vol. 21(2). – P. 34–42.
8. Mosenia A. A survey on security in Internet of Things: State of the art and challenges / A. Mosenia, N. K. Jha // *Computer Networks*. – 2017. – Vol. 111. – P. 17 – 48.
9. Sicari S. Security, privacy and trust in Internet of Things: The road ahead / S. Sicari, A. Rizzardi, L. Grieco, A. Coen-Porisini // *Computer Networks*. – 2015. – Vol. 76. – P. 146 – 164.
10. Kulkarni A. “Modeling Traffic with BMAP Queues for Performance Analysis of IoT Networks” *International Journal of Computer Applications*, vol. 182, no. 2, pp. 12 – 18, 2018.

REFERENCES:

1. Andriychuk M. Traffic modeling in Internet of Things networks / M. Andriychuk // *Radioelectronics, Informatics, Management*. – 2020. – No. 2. – P. 15 – 23.
2. Kovalchuk V. Features of using the MQTT protocol in IoT / V. Kovalchuk, I. Ivanova // *Scientific works of ONAZ named after O. S. Popov*. – 2019. – No. 4. – P. 56 – 62.
3. Lapko A. Simulation modeling of IoT network protection / A. Lapko, S. Prytula // *Bulletin of NTUU "KPI". Series: Informatics and computing*. – 2021. – No. 75. – P. 44 – 50.
4. Hrytsenko V. Approaches to building IDS for IoT / V. Hrytsenko, M. Solovey // *Information Processing Systems*. – 2022. – No. 3(172). – P. 27 – 34.

5. Melnyk O. Using Markov processes to describe IoT traffic / O. Melnyk // Mathematical modeling and computational methods. – 2020. – Vol. 2, No. 1. – P. 91 – 99.
6. Chen S. A survey on industrial Internet of Things security architecture / S. Chen, H. Xu, D. Liu et al. // Future Internet. – 2020. – Vol. 12(1). – P. 1 – 18.
7. Alrawais A. Fog computing for the Internet of Things: Security and privacy issues / A. Alrawais, A. Alhothaily, C. Hu, X. Cheng // IEEE Internet Computing. – 2017. – Vol. 21(2). – P. 34 – 42.
8. Mosenia A. A survey on security in Internet of Things: State of the art and challenges / A. Mosenia, N. K. Jha // Computer Networks. – 2017. – Vol. 111. – P. 17 – 48.
9. Sicari S. Security, privacy and trust in Internet of Things: The road ahead / S. Sicari, A. Rizzardi, L. Grieco, A. Coen-Porisini // Computer Networks. – 2015. – Vol. 76. – P. 146 – 164.
10. Kulkarni A. “Modeling Traffic with BMAP Queues for Performance Analysis of IoT Networks” *International Journal of Computer Applications*, vol. 182, no. 2, pp. 12 – 18, 2018.

Dr. Tech. Sci., prof. Khlaponin Yu.I., Kondakova A.M.

RESEARCH ON THE EFFECTIVENESS OF DEVELOPED ALGORITHMS AND PROTECTION MODELS IN INTERNET OF THINGS NETWORKS

The article considers approaches to ensuring high-quality service of Internet of Things (IoT) services in 5G networks, taking into account modern challenges in terms of scalability, variable topology and security threats. Considerable attention is paid to modeling IoT traffic, building mathematical service models and assessing parameters that affect the level of reliability and timeliness of data delivery.

During the study, the specifics of the structure of IoT networks were analyzed, key traffic metrics were identified and a mathematical model was built based on the classical Poisson model, as well as its extensions MMPP and BMAP to adequately reflect the variable and clustered traffic structure in IoT networks. Clustering was performed using the k-means algorithm to profile normal node behavior, which made it possible to detect anomalies in real time. A formal risk assessment model was proposed that takes into account deviations of current metrics from a typical cluster and changes in intensity. An adaptive incident response mechanism with threshold values that determine the level of intervention from limiting activity to completely blocking the device. For verification, DDoS, device substitution, and stealth attack scenarios were simulated. The effectiveness of the detection algorithm was assessed using the metrics precision, recall, F1-score, and response time.

The results showed that the proposed methodology provides high anomaly detection accuracy (F1-score = 92.5%) with a response time of up to 80 ms, which makes it suitable for use in real IoT systems. The proposed approach allows for increased network reliability and security without significantly increasing computational costs. The findings confirm the feasibility of implementing intelligent monitoring systems based on clustering and risk models in the 5G-IoT infrastructure.

Keywords: *internet of Things, traffic modeling, cybersecurity, protection algorithms, 5G, IDS, anomalies.*

ЗАГАЛЬНІ ПИТАННЯ

УДК 355.1:351.86(569.4)

д. н. держ. упр., проф. Акімов О.О. (МОУ)
Золотов А.В. (НУОУ)
Андрусяк М.В. (МОУ)
Русецький Р.Ю. (МОУ)

DOI: <http://doi.org/10.17721/2519-481X/2025/88-10>

АНАЛІЗ ДОСВІДУ ФОРМУВАННЯ ВІЙСЬКОВОГО ЗАКОНОДАВСТВА ЩОДО ПРОХОДЖЕННЯ ВІЙСЬКОВОЇ СЛУЖБИ У ЗБРОЙНИХ СИЛАХ ІЗРАЇЛЮ

Анотація. У статті здійснено комплексний аналіз досвіду формування військового законодавства Ізраїлю щодо проходження військової служби, для виявлення його потенційної прикладної цінності для реформування відповідної нормативно-правової бази в Україні. На основі міждисциплінарного підходу, з використанням методів порівняльно-правового аналізу, нормативного моделювання та структурної оцінки оборонного законодавства, охарактеризовано ключові засади кадрової політики Армії оборони Ізраїлю (ЦАХАЛ), зокрема щодо загального призову, резервної служби, соціальних компенсаторів, гендерної інтеграції, судового та парламентського контролю. Проаналізовано чинне ізраїльське законодавство у сфері військової служби, зокрема Закон про службу в ЦАХАЛ, поправки 2024-2025 рр. до нього, судову практику Верховного суду Ізраїлю та рішення Кнесету щодо подовження строків служби і посилення резервної участі. Узагальнено практичні кейси: запуск спеціалізованих підрозділів для релігійних груп, механізм компенсацій втрати доходу, впровадження цифрових реєстрів навичок резервістів, а також автоматизоване відшкодування з боку Національного інституту страхування. Показано ефективність правових інструментів, спрямованих на збереження мобілізаційної стійкості та суспільної легітимності служби в умовах тривалого збройного конфлікту. Проведено порівняльний аналіз українського та ізраїльського військового законодавства, виявлено нормативні прогалини у вітчизняному регулюванні, зокрема: відсутність консолідованого рамкового закону, чітких строків служби для мобілізованих, стабільної системи пільг для резервістів, механізму альтернативної служби у воєнний період та незалежного органу правового нагляду. На основі дослідження сформульовано висновок про доцільність адаптації ключових елементів ізраїльської моделі – цифрових платформ, соціальних гарантій, подвійного парламентсько-судового контролю та стандартів гендерної інтеграції. Стаття доводить, що ізраїльський досвід у сфері військового законодавства демонструє високий рівень нормативної гнучкості, оперативної адаптації до змін безпекового середовища, балансу між загальним обов'язком і соціальними компенсаціями, а також стійкості у політичних конфліктах. Українська модель може бути ефективно трансформована за умови уніфікації законодавства, впровадження стратегічного планування кадрової політики, інституційної послідовності та підвищення рівня демократичного контролю.

Ключові слова: військове законодавство, військова служба, мобілізація, резерв, соціальні гарантії, sunset-клаузи, альтернативна служба, парламентський контроль, ЦАХАЛ, військова юстиція, Україна, порівняльний аналіз.

Постановка проблеми. В умовах тривалих загроз національній безпеці та військово-політичної нестабільності в регіоні, Ізраїль сформував унікальну модель військового законодавства, що поєднує загальний обов'язок служби, гнучкі механізми резервної підготовки та високий рівень інтеграції армії в суспільне життя. Водночас Україна, яка перебуває у стані воєнної загрози, стикається з проблемами неефективної нормативно-правової бази у сфері проходження військової служби, фрагментарністю законодавства та відсутністю єдиної доктрини кадрової політики оборонного сектору. Концептуальні підходи до аналізу та прогнозування загроз національній безпеці, запропоновані М. Миколайчуком та

співавторами (2025) [1], підтверджують, що ефективність оборонної політики ґрунтується на agile-моделі права, здатній швидко реагувати на динаміку ризиків.

Попри актуалізацію військового законодавства у післявоєнний період, в Україні досі відсутній системний підхід до вдосконалення правових засад проходження служби в умовах гібридної війни та мобілізаційної трансформації суспільства. Це вимагає вивчення ефективних моделей інших держав, зокрема Ізраїлю, який, маючи тривалу історію збройного протистояння, розробив нормативно-правові механізми, що забезпечують стабільність комплектування збройних сил, ефективне управління людськими ресурсами та баланс між військовими обов'язками й демократичними правами громадян.

Аналіз досвіду Ізраїлю є важливим для розуміння того, як військове законодавство може стати чинником національної стійкості, адаптивності та інтеграції оборонної політики у систему публічного управління України.

Аналіз останніх досліджень і публікацій. Аналіз останніх досліджень і публікацій підтверджує, що ключовим чинником ефективного функціонування військової системи Ізраїлю є її адаптивність до викликів безпеки, демократичний контроль та високий рівень аналітичного супроводу. М. В. Андрусак, Р. Ю. Русецький та О. О. Акімов (2025) [2] розглядають поліграф як складову кадрової політики у сфері національної безпеки, підкреслюючи важливість міждисциплінарного підходу до формування персоналу, що особливо актуально в контексті роботи з резервістами. Законодавчі ініціативи Ізраїлю щодо резерву охоплюють комплексний захист прав військовослужбовців, про що свідчить аналіз А. Гарель (2024) [3] стосовно відмов резервістів на тлі судової реформи, а також документ Military Justice System [4], що засвідчує дотримання процесуальних гарантій. Законодавчі аналітичні висновки, надані Israel Democracy Institute [5], деталізують правові наслідки змін у тривалості як обов'язкової, так і резервної служби. Практичні аспекти цифровізації мобілізаційних процесів розглядаються в офіційному джерелі Mitgaisim (2023) [6], де йдеться про платформу «Tzav Rishon» як ключовий інструмент первинного відбору. Додатково, платформа miluim.idf.il, яка аналізується на ресурсі AhrefsTop (2025) [7], ілюструє можливості автоматизованого обліку резервістів, цифрових посвідчень і готовності до виклику. Культурно-соціальні виклики служби розкриває публікація С. Шаффе (2024) [8], яка описує спробу законодавчого врегулювання військового обов'язку ультраортодоксальних євреїв, а також репортажі Times of Israel (2025) [9; 10; 11], що аналізують участь жінок та літніх резервістів у бойових діях. Аналітичну картину доповнюють результати соціологічного опитування INSS (2025) [12], згідно з якими рівень довіри до армії залишається стабільно високим попри політичні суперечності.

Узагальнюючи, варто відзначити, що успішність ізраїльської моделі полягає у поєднанні гнучкого нормативного регулювання, технологічної модернізації обліку та інклюзивного підходу до військового обов'язку, що підтверджується практиками Prime Minister's Office (2025) [12] і Military Advocate General's Corps [4].

Мета дослідження полягає в аналізі ізраїльського досвіду формування військового законодавства щодо проходження служби та визначенні можливостей його адаптації для України. Основна увага приділена розробленню рамкового закону про військову службу, унормуванню строків мобілізації, цифровізації військового обліку та впровадженню демократичного контролю й індексованих соціальних гарантій для резервістів.

Методологія дослідження. У процесі аналізу було використано порівняльно-правовий аналіз, що дозволив зіставити ізраїльську нормативно-правову базу з українською в частині регламентації військового обов'язку, проходження служби, резерву, пільг та контролю з боку парламенту й судової системи. Метод контент-аналізу використовувався для систематизації ключових тез ізраїльських урядових та аналітичних документів (зокрема сайту Mitgaisim, законодавчих актів Кнесету, експертних висновків Інституту національної безпеки Ізраїлю, Belfer Center та інших), що дало змогу ідентифікувати головні тренди нормативних змін 2023-2025 років. Інституційний аналіз був використаний для вивчення організаційної побудови системи кадрового резерву Ізраїлю, функцій таких структур, як Meitav, Aman,

Управління мобілізації, та їх цифрового забезпечення, що дозволило оцінити сталість і гнучкість даної системи. Метод кейс-стаді дозволив вивчити прикладну практику реалізації цифрової платформи обліку резервістів та індексів готовності на базі ЦАХАЛ, її технічні компоненти, що є релевантним до потреб реформування військового обліку в Україні. Метод нормативного моделювання застосовувався для формування концептуальної пропозиції щодо створення в Україні уніфікованого цифрового аналітичного профілю резервіста, що враховує як військово-облікові, так і психофізіологічні характеристики особи.

Виклад основного матеріалу. В умовах затяжної воєнної загрози та соціальної мобілізації Ізраїль виробив багаторівневу систему правового регулювання військової служби, що поєднує загальний призов, потужний резерв і низку соціальних компенсаторів. ЦАХАЛ охоплює сухопутний, повітряний і морський компоненти під єдиним генеральним штабом, що забезпечує швидке інтегроване реагування на кризові сценарії [13]. Базовий строк обов'язкової служби для чоловіків становить 32 місяці, для жінок – 24 місяці. Водночас у 2024 році Кнесет схвалив тимчасову поправку, що подовжує службу до трьох років, аби компенсувати зростаючий дефіцит особового складу [14]. На нашу думку, дана норма демонструє гнучкість законодавця, однак потребує чітких соціальних гарантій, аби не поглибити дисбаланс обов'язків між різними групами населення.

Принагідно зауважити, що резервна система ґрунтується на поетапному залученні демобілізованих військовиків до 40 років, що дає змогу швидко наростити бойову спроможність. У червні 2024 року уряд підтримав законопроект, який відкладає вік виходу з резерву, мотивуючи це необхідністю втримати досвідчені кадри [9]. Паралельно держава розширила пільги для резервістів: житлові гранти та податкові знижки стали стимулом для збереження їхньої мотивації [15]. Ми частково погоджуємося з оцінкою ізраїльських аналітиків, що подібна економічна стабільність підвищує боєздатність війська, але без збалансованого громадянського контролю ризикує перетворитися на прихований податковий тягар.

Судове рішення Верховного суду Ізраїлю 25 червня 2024 року демонструє ключовий поворот в політиці. Так, М. Шаффе зазначив, що уряд не має права звільняти студентів єшив (хареді) від обов'язкового призову, і зобов'язав припинити фінансування тих навчальних закладів, чиї вихованці не служать у армії [8]. Однією з практичних імплементацій стало формування спеціалізованого підрозділу – «Хасмонеїська бригада» – для хареді, де враховано їх релігійний спосіб життя: суворе дотримання єврейських побожних практик, обмеження медіа, молитви, навчання Тори у службовому графіку [12].

Дані кейси підтверджують нашу позицію: комплектування не може спиратися виключно на моральну мотивацію більшості, якщо привілейована група звільняється від обов'язку. Натомість, впровадження цілеспрямованих програм адаптації (як-от окремі бригади або етапні програми) та рішуче судове втручання здатні мінімізувати розрив між безпековими потребами та соціальною згуртованістю.

Гендерний вимір військового законодавства у Ізраїлі відзначається динамічними реформами. У 2024 році ЦАХАЛ відкрив пілотні програми для жінок у спецпідрозділах «669», «Саєрет Маткаль» та «Ягалом», що збільшило питому вагу жінок у бойових ролях до 20% [10]. Водночас Кнесет у 2025 році розглядає законопроект про закріплення прав жінок-військовослужбовиць і одночасну інтеграцію хареді, що підкреслює спробу збалансувати гендерну рівність з релігійними потребами [16]. Р. Мазалі фіксує тенденцію до зниження загальної явки призовників, попри лібералізацію правил залучення жінок [17]. Ми частково погоджуємося з автором, додаючи, що сам факт розширення жіночої участі не компенсує структурних демографічних викликів.

Отже, ізраїльський досвід підтверджує, що ефективність військового законодавства визначається поєднанням таких ключових факторів:

– *нормативна гнучкість щодо строків служби та резерву*: законодавство Ізраїлю дозволяє адаптувати терміни та умови проходження військової служби залежно від віку, сімейного статусу, релігійних переконань та професійної підготовки. Це особливо

проявляється у таких програмах, як «Шлав Бет» для хареді або короткострокові офіцерські курси для спеціалістів. Такі механізми створюють гнучку, але контрольовану систему призову й резерву, орієнтовану на стратегічні потреби;

– *адресні соціальні компенсації*: Ізраїль надає широкий спектр пільг для військовослужбовців і ветеранів: від фінансових бонусів за службу до пільг на навчання, іпотеку, медичне забезпечення та адаптаційні програми після демобілізації. Особливі умови передбачені для представників релігійних громад, багатодітних сімей та учасників бойових дій. Такий підхід зміцнює суспільну підтримку інституту служби й формує мотиваційний потенціал;

– *принцип «спільного обов'язку» без дискримінаційних винятків*: у центрі ізраїльської системи захист держави, який є справою всіх громадян, незалежно від їх етнічного, релігійного чи соціального статусу. Водночас держава пропонує адаптаційні механізми, як-от створення окремих підрозділів, що забезпечують можливість служити без порушення релігійних норм та сприяють зниженню соціальної напруги, збереженню легітимності загального призову, забезпечуючи інклюзивність без прямого примусу.

Для України, котра реформує власну модель комплектування в умовах гібридної війни, доцільно адаптувати саме механізм балансування обов'язків і пільг, запровадивши диференційовані, але обов'язкові форми залучення громадян до сектору оборони, а також посилити контроль Верховної Ради над реалізацією військових законів, аналогічно до ролі Кнесету.

Нормативно-правова архітектура, що регулює проходження військової служби в Ізраїлі, вибудована за принципом єдиного рамкового закону + спеціальних поправок, що оперативно реагують на зміну безпекового середовища. Центральним актом є Закон про службу в Армії оборони Ізраїлю (консолідована редакція 1986 р.), до якого у липні 2024 року Кнесет ухвалив поправку, що продовжила строк обов'язкової служби для чоловіків із 32 до 36 місяців, обґрунтовуючи це дефіцитом особового складу та необхідністю зменшити навантаження на резервістів [18]. Паралельно уряд підтримав меморандум до Закону про резервну службу, який підвищує граничний вік перебування у строю та збільшує максимальну тривалість щорічних зборів. Ми погоджуємося із меморандумом щодо посилення мобілізаційної спроможності, однак зазначаємо ризик перевантаження сімей резервістів, якщо не поширити адресні пільги.

Станом на серпень 2024 року Ізраїль запровадив системні соціальні гарантії для резервістів та їхніх родин, що формалізовано тимчасовим приписом до Закону про національне страхування. Зокрема, припис поширюється до 31 грудня 2024 року (з можливим продовженням), і встановлює наступні ключові пільги: заборона на звільнення або неоплачувані відпустки для подружжя резервіста без письмового дозволу Комітету з працевлаштування; право подружжя на право добору компенсації на рівні допомоги з безробіття; заборона врахування періоду резервної служби до тривалості трудового стажу; можливість накладати фінансові санкції на роботодавця у разі порушення цих гарантій [5].

Як практичний кейс: суб'єкт господарювання, який наприкінці серпня 2024 року ініціював звільнення подружжя резервіста під час навчальних зборів, був зобов'язаний Комітетом з працевлаштування поновити працівницю та оплатити компенсацію – рішення ґрунтувалося саме на цьому нововведенні [5]. Це чітко ілюструє дієвість механізму і його потенційну реальну користь сім'ям військовослужбовців.

Окрім цього, ізраїльський фонд «Бітюах Леумі» (Національний інститут страхування) починаючи з 2023-2024 років автоматично виплачує резервістам для самозайнятих компенсації за втрачений дохід – мінімальна сума сягає приблизно NIS 321.07 на день, а максимальна межа – близько NIS 1 689.83, залежно від доходів попереднього періоду. Для найманих працівників компенсацію виплачує роботодавець, але фонд відшкодовує різницю у випадку перевищення межі через спеціальний трансфер, і це здійснюється без необхідності самостійного оформлення претензії [19], що означає – ізраїльська система гарантує

непродовжувану зарплату резервістам, навіть якщо вони не мають можливості передати документи до фонду – виплата часто здійснюється автоматично та ретроспективно. Таким чином, роботодавцю необхідно надавати стандартну оплату, а фонд компенсує витрати без додаткового навантаження на резервіста.

Вищезазначені кейси доводять, що ізраїльська модель забезпечує правовий захист для сімей резервістів, гарантований дохід та швидке автоматизоване відшкодування, що не вимагає складної бюрократії.

У нашій оцінці, зазначена модель є «необхідною компенсацією», як зазначає Р. Левуш [20], але ми відзначаємо: аби уникнути перетворення на лакуну фінансової нестабільності, потрібне сталий фінансовий фундамент. Зокрема, створення резервного фонду, довгострокове бюджетне планування й обґрунтована індексація витрат на виплати резервістам – ті елементи, що запобігатимуть перетворенню пільг на невиправданий фінансовий тягар у разі подовження мобілізаційної кампанії.

Важливим елементом системи є судово-правові запобіжники. У листопаді 2024 року Верховний суд постановив, що уряд не має повноважень звільняти студентів вишив від служби та зобов'язав припинити бюджетування закладів, чиї вихованці не призиваються. Дане рішення посилює позиції світських партій у дискусії про рівність обов'язків і підштовхнуло Кабінет міністрів до пошуку компромісу, адже відставка ультраортодоксальних фракцій у липні 2025 р. майже зруйнувала правлячу коаліцію [21]. Ми частково згодні з авторами, які вбачають у судовому втручанні «інструмент забезпечення загальної відповідальності», та уточнюємо, що воно одночасно підвищує ризик політичної дестабілізації оборонної політики країни.

Регулятивні повноваження розподілено між кількома інституціями. Кнесет затверджує закони та контролює їх виконання через профільний комітет з іноземних справ та оборони. Міністерство оборони видає накази-виконавчі інструкції, тоді як Корпус військового адвоката (прокуратура ЦАХАЛ) здійснює правовий нагляд над дотриманням дисциплінарних норм і надає правову експертизу кожному підрозділу [4]. Праця А. Гареля про відмову резервістів служити у контексті конституційної реформи демонструє, що саме ефективність прокуратури мінімізує кількість судових позовів щодо порушення прав військовослужбовців [3]. Ми погоджуємося з автором і додаємо, що сильна внутрішня юстиція знижує навантаження на цивільні суди та підсилює демократичний контроль. М. Андрусяк, О. та автори доводять, що додатковим запобіжником від ризиків у ЦАХАЛ виступає поліграф-скринінг при оформленні допуску до військових посад [2]. Невдале проходження тесту автоматично блокує доступ до секретної інформації. Процедура спирається на мережу сертифікованих поліграфологів, які проходять понад 400 годин міждисциплінарної підготовки за стандартами NCCA/APA з акцентом на моделювання контрзаходів, етику та правові обмеження [2].

Узагальнюючи для українського контексту, слід адаптувати механізм подвійного парламентсько-урядового контролю та створити автономний корпус військової юстиції з повноваженнями попереднього правового аудиту наказів. У поєднанні з адресними пільгами це дозволить підвищити прозорість, довіру суспільства й стійкість кадрового комплектування.

Після ухвалення поправок 2024-2025 рр. оборонна система Ізраїлю отримала відчутні практичні результати, що вимірюються не лише чисельністю особового складу, а й рівнем громадської легітимації та здатністю витримувати затяжні конфлікти. Подовження обов'язкової служби для чоловіків до 36 місяців забезпечило додатково близько 9 тис. військовослужбовців на цикл призову, що дало змогу скоротити щорічний дефіцит кадрів удвічі. Одночасно різке зростання резервної активності +50% резервістів віком понад 50 років в умовах війни у Секторі Гази підтвердило гнучкість та мобілізаційну стійкість системи, хоча спричинило дебати щодо довгострокового навантаження на сім'ї [11].

Попри окремі сигнали кадрового виснаження – 14600 зареєстрованих ухильників і пропозиції залучати діаспору – рівень довіри суспільства до ЦАХАЛ залишається домінуюче

високим: травневі опитування INSS зафіксували 75,5% підтримки, а червні – 82% [22]. Ми частково погоджуємось із тезою про схильність громадян підтримувати армію, коли інші інституції демонструють слабкість, та підкреслюємо, що стабільний авторитет ЦАХАЛ є критичним буфером для виконання жорстких мобілізаційних рішень.

Показник стійкості до тривалих загроз вимірюється індикаторами національної резильєнтності. Звіт INSS «State of National Resilience – Operation Rising Lion» демонструє збереження позитивної динаміки соціальної згуртованості попри 20-місячну війну, але вказує на ризик «поляризаційного перелому» за збереження високого податкового навантаження на резервістів [23]. Наша позиція полягає у підтримці рекомендації авторів щодо негайного перегляду моделі пільг, щоби запобігти «втомі служби» та втраті кадрового ресурсу, що вже проявляється у вибіркових відмовах резервістів повторно вирушати на фронт.

Отже, ізраїльський підхід забезпечив відносно ефективне комплектування й високу підтримку армії навіть у затяжному конфлікті, однак його подальша дієвість залежить від балансування фіскальних витрат і соціальних пільг. Для України ключовим уроком є поєднання чисельного нарощування з постійним моніторингом громадської довіри та адаптивним коригуванням компенсацій, щоб забезпечити кадрову стійкість у довготривалому протистоянні.

Варто підкреслити, що цифрова трансформація мобілізаційних і призовних процесів в Ізраїлі відбувається за логікою інтегрованої кадрової екосистеми, де кожен етап – від первинного відбору до ротаций резервістів – підтримується єдиним інформаційним контуром. Первинний скринінг кандидатів здійснюється через онлайн-платформу *Tzav Rishon*, що поєднує дистанційні комп'ютеризовані тести та медичні анкети; результати одразу надходять до бази даних підрозділу Meitav (Енлістмент-центр ЦАХАЛ), який формує персональні траєкторії служби та автоматично призначає дату явки [6].

Для резерву працює портал miluim.idf.il з особистим «кабінетом» військовозобов'язаного: тут зберігаються цифрові посвідчення, історія зборів, навички, медичні довідки та прогноз доступності; система надсилає push-сповіщення про *Tzav 8* (екстрений виклик) і формує довідки для роботодавця [7]. Дані підтягуються до централізованого ERP-ядра “Merkava-HR” (SAP-орієнтований модуль кадрового обліку), а для тактичного планування бойових посад використовується модуль “Milonit”, в якому офіцери резерву відзначають наявні компетенції та проходження курсів.

Аналітика навичок ґрунтується на чотирьох показниках: кваліфікаційний ранг, рівень бойового досвіду, медико-психологічна придатність і індекс доступності (число днів, упродовж яких резервіст може бути відсутній на цивільній роботі). Після кожних зборів ці показники оновлюються автоматично через мобільний застосунок, що мінімізує паперовий документообіг і забезпечує актуальність профілів.

В українському контексті важливо розглядати цифрову трансформацію мобілізаційних і призовних процесів не лише як технічне оновлення, а як формування єдиної кадрової екосистеми оборони, що забезпечує прозорість, швидкість реагування та прогнозування людських ресурсів. На даному етапі в Україні вже запроваджено проєкт «Резерв+», який створює цифрові особисті кабінети для військовозобов'язаних і дозволяє вести їхній облік онлайн. Проте потенціал системи може бути суттєво розширений, якщо інтегрувати в неї практики, апробовані в ЦАХАЛі. Ключовими передумовами є: уніфікація стандартів даних, незалежний кібер-аудит системи та чіткий розподіл доступів між Міноборони, Мінцифри, МОЗ і ДПС. Така логіка відповідає підходу ЦАХАЛу, що реалізується у межах Momentum-архітектури, але має бути адаптована до українських реалій.

Задля виявлення релевантних механізмів удосконалення національного військового законодавства доцільним є систематичне порівняння нормативно-правових моделей Ізраїлю та України. Ізраїль, як держава з хронічним станом безпекової загрози, сформував адаптивну, соціально збалансовану та юридично обґрунтовану систему проходження військової служби. Україна, яка перебуває у стані широкомасштабної війни, запровадила низку актуальних змін,

однак її нормативна база все ще демонструє фрагментарність, нестачу системності та прозорості. Порівняльна таблиця дозволяє виявити ключові точки перетину та розриву між двома підходами, а також окреслити наявні правові прогалини в українському законодавстві (табл. 1).

Таблиця 1

Порівняльний аналіз військового законодавства Ізраїлю та України щодо проходження військової служби: спільні риси, відмінності та правові прогалини

Критерій	Ізраїль	Україна	Спільне / відмінне	Нормативно-правові прогалини в Україні
Рамковий закон	Закон про службу в Армії оборони Ізраїлю	Закон «Про військовий обов’язок і військову службу»	Обидві системи спираються на базовий закон із численними поправками	Немає консолідованої редакції; норми розпорошені в десятках актів
Тривалість обов’язкової служби	36 міс чоловіки, 24 міс жінки (тимчасова норма з 2024)	мобілізовані служать без встановленого ліміту; призовний вік знижено до 25 років	Загальний призов існує в обох країнах	Відсутня максимальна тривалість служби під час мобілізації → складно планувати оборонний кадровий цикл
Резерв	Обов’язковий резерв до 41 року (солдати) / 46 років (офіцери)	Оперативний резерв I–III до 60 років	Обидві моделі покладаються на резерв	Немає чіткої системи планових зборів, квот і гарантованого пакета пільг
Альтернативна та релігійна служба	Звільнення хареді у 21 років; механізми національної служби	Закон про альтернативну службу діє, але під час воєнного стану право фактично призупинене	Обидві системи декларують альтернативу	Відсутні робочі процедури реалізації права на альтернативу під час мобілізації
Соціальні гарантії	Податкові знижки, житлові гранти, компенсація втрати доходів резервістів	Разові виплати й підвищена зарплата; нові пільги 2025 стосуються повернення резервістів	Фінансові стимули застосовують обидві країни	Пільги не системні, відсутня індексація та стабільне фінансування
Гендерна інтеграція	Жінки в бойових підрозділах, частка ≈ 20%	Розширено перелік спеціальностей (2022-2024), але немає окремої програми підтримки	Обидві країни розширюють участь жінок	Немає стандартів оснащення, медзабезпечення та соцупроводу для військовослужбовиць
Цивільний контроль	Комітет Кнесету + автономний корпус військової прокуратури	Парламентський комітет існує, але немає інституційного військового омбудсмена з аудитом наказів	Обидві моделі мають парламентський нагляд	Відсутній незалежний корпус військової юстиції з превентивним контролем
Гнучкість поправок	Тимчасові положення з автоматичним переглядом через 2 роки	Продовження мобілізації кожні 90 днів	Закони часто коригуються в обох країнах	Немає інструменту ex-ante оцінки впливу правок.

Авторська розробка.

Проведене порівняння доводить, що обидві країни демонструють прагнення до розбудови адаптивної, гнучкої та соціально орієнтованої системи проходження військової

служби. Однак ізраїльське військове законодавство значно випереджає Україну у впровадженні структурованих рішень, які поєднують безпекові пріоритети із соціальними компенсаціями та демократичним контролем. Україна потребує уніфікації правового поля, консолідації строків служби, посилення гарантій для резервістів, незалежного механізму юридичного нагляду та системного моніторингу ефективності впроваджених норм. Запозичення ізраїльського досвіду має відбуватися з урахуванням національних реалій, однак саме він дає змогу сформулювати принципи ефективної кадрової мобілізаційної політики у період довготривалого воєнного протистояння.

Аналіз ізраїльської моделі формування військового законодавства дозволяє виокремити низку конструктивних елементів, які можуть бути адаптовані в українському контексті з урахуванням реалій тривалого збройного конфлікту. Запропоновані нижче рекомендації ґрунтуються на структурних характеристиках правової моделі ЦАХАЛ та враховують виявлені нормативно-правові прогалини в українському законодавстві.

Доцільним є запровадження в Україні рамкового закону про військову службу з інституту націоналізованими тимчасовими положеннями (sunset-клаузами), що автоматично переглядаються після закінчення визначеного строку. Ізраїльська практика продовження строку обов'язкової служби за допомогою обмежених у часі поправок, що супроводжуються парламентським контролем, довела свою ефективність у забезпеченні балансу між воєнною необхідністю та соціальною передбачуваністю. Для України це означає потребу фіксації чітких термінів дії мобілізаційних норм, їх аудиту за результатами впровадження та закріплення прозорих критеріїв пролонгації або згортання.

Другим пріоритетом має стати унормування строків проходження служби для мобілізованих осіб, включаючи передбачувану циклічність (служба – відпустка – повторне залучення). Упровадження чітких строків служби, аналогічно до ізраїльських механізмів, сприятиме підвищенню довіри до державної мобілізаційної політики та зменшенню соціального напруження.

Третім важливим кроком має бути структурна реформа резерву. Вона повинна охоплювати встановлення граничного віку участі, чітке нормативне регулювання кількості днів зборів, створення гарантованого пакета пільг для резервістів та працедавців, а також розгортання єдиного цифрового реєстру навичок і стану бойової готовності резервного складу. та розгортання єдиного цифрового реєстру навичок і стану бойової готовності резервного складу. При цьому, як показує дослідження М. Миколайчука та інших науковців, ефективність таких платформ різко зростає, коли вони інтегровані в agile-цикл аналізу й прогнозування загроз національній безпеці, що забезпечує оперативне коригування мобілізаційної політики в режимі «near-real-time» [1]. Ізраїльський досвід демонструє: мобілізаційна гнучкість досягається лише у поєднанні з прогнозованістю та соціальною підтримкою.

Соціальний пакет резервістів має бути не лише зафіксований у законодавстві, а й підлягати автоматичній індексації з огляду на інфляцію та тривалість виконання обов'язків. В Ізраїлі фінансова компенсація втрати доходів, податкові пільги, житлові гранти створюють сприятливе середовище для збереження боєздатного резерву. Впровадження аналогічного підходу в Україні дозволить зменшити «втому служби» та підвищити мотивацію військовозобов'язаних.

Важливим елементом є запровадження подвійного демократичного контролю – з боку парламенту та незалежного органу військової юстиції. На прикладі Ізраїлю показово, що рішучі втручання Верховного суду щодо зловживань виконавчої влади стали ключовим механізмом захисту принципу загального обов'язку. Україна може імплементувати подібний підхід шляхом створення автономного корпусу військової юстиції, уповноваженого на здійснення превентивного правового аудиту рішень у сфері оборони.

Гендерна інтеграція потребує переходу від декларативних до нормативно врегульованих стандартів. Доцільним є розроблення окремих нормативних актів, які регламентують оснащення, медичне забезпечення, гігієнічні умови та фізичну підготовку

жінок-військовослужбовиць. Ізраїльський досвід свідчить, що активна участь жінок у бойових підрозділах можлива лише за умов цілеспрямованої інституційної підтримки.

Окремої уваги потребує правове регулювання альтернативної (невійськової) служби під час воєнного стану. Україна має сформувати чіткий, індивідуально орієнтований і юридично контрольований механізм реалізації цього права, який не створюватиме привілеїв для окремих соціальних чи релігійних груп, а відповідатиме стандартам демократичної рівності.

Нарешті, доцільним є створення відкритої системи моніторингу ефективності військового законодавства та мобілізаційної політики. Йдеться про регулярну публікацію аналітичних звітів щодо комплектування, плинності кадрів, впливу законодавчих змін на ринок праці та рівень довіри до армії. Саме такий інструмент уможливило своєчасне коригування політик і підвищення прозорості сектору безпеки.

Очікувані бар'єри при впровадженні ініціатив можуть мати правовий, інституційний, фінансовий та політичний характер. Зокрема, фрагментарність законодавства й конкуренція повноважень між відомствами ускладнюють уніфікацію норм, а обмеженість фінансових ресурсів – реалізацію комплексної системи пільг. Крім того, політичні ризики, пов'язані зі спробами групового уникнення служби, можуть призвести до втрати суспільної легітимності мобілізації. Вирішення цих проблем вбачається у створенні міжвідомчої кодифікаційної групи, поступовому впровадженні нових норм через пілотні моделі, трирічному бюджетному плануванню й чіткому контролю над наданням будь-яких винятків.

Таким чином, ізраїльський досвід може бути ефективно адаптований в Україні за умови стратегічного мислення, інституційної послідовності та забезпечення балансу між оборонними потребами, правами людини та соціальною справедливістю.

Висновки та пропозиції. Аналіз ізраїльського досвіду у сфері нормативно-правового регулювання проходження військової служби засвідчує, що ефективність мобілізаційної політики на пряму залежить від здатності правової системи забезпечити гнучке реагування на загрози, соціальну передбачуваність та демократичну легітимність. В умовах затяжного збройного протистояння Ізраїль сформував унікальну правову модель, що базується на поєднанні рамкового закону та оперативних поправок, інтеграції безпекових і соціальних аспектів, розвитку адресної підтримки резервістів і реалізації дворівневого контролю з боку парламенту та судової влади. Судові рішення щодо забезпечення рівності призову, розширення участі жінок у бойових підрозділах, автоматизація компенсацій резервістам, а також створення спеціалізованих механізмів для релігійних груп свідчать про високий ступінь адаптивності та правової обґрунтованості даної моделі.

У контексті України, яка знаходиться у стані повномасштабної війни, виявлено низку правових прогалин: фрагментарність нормативної бази, відсутність фіксованих строків служби для мобілізованих, недостатня соціальна підтримка резервістів, слабкий превентивний контроль за оборонними рішеннями та нерегламентована система альтернативної служби. У цьому зв'язку доцільним є розроблення консолідованого рамкового закону про військову службу з sunset-клаузами, які підлягають обов'язковому перегляду після визначеного терміну дії. Важливим кроком є унормування передбачуваних строків служби для мобілізованих осіб з урахуванням циклічності та забезпечення балансу між службою і цивільним життям.

Необхідною є структурна реформа резерву, яка включає визначення граничного віку, регламентацію кількості днів зборів, гарантовані пільги для резервістів та роботодавців, а також створення цифрового реєстру бойової готовності особового складу. Соціальний пакет резервістів має бути індексований та автоматично оновлюваний, виходячи з тривалості служби та фінансових викликів. З метою підвищення прозорості та довіри до військової політики слід впровадити демократичний контроль у формі подвійного нагляду: з боку парламенту та автономного корпусу військової юстиції з правом превентивного аудиту оборонних рішень. Для підвищення ефективності мобілізаційної політики необхідно створити публічну систему моніторингу її результативності, яка б забезпечувала регулярне

оприлюднення даних щодо комплектування, кадрової плинності, впливу на ринок праці та рівень довіри до армії.

Отже, ізраїльська модель військового законодавства може бути ефективно адаптована в Україні за умови стратегічного мислення, нормативної узгодженості, фінансової сталості та пріоритетності суспільної довіри в процесах оборонного управління.

ЛІТЕРАТУРА:

1. Mykolaichuk, M., Petrukha, N., Akimova, L., Pozniakovska, N., Hudenko, B., & Akimov, O. (2025). Conceptual principles of analysis and forecasting threats to national security in modern conditions. *Sapientia: International Journal of Interdisciplinary Studies*, 6(2), e25029. DOI: <https://doi.org/10.51798/sijis.v6i2.985>
2. Андрусак М. В., Русецький Р. Ю., Акімов О. О. Поліграф у системі національної безпеки: міждисциплінарні підходи до підготовки кадрів та зарубіжна практика. *Національні інтереси України*. 2025. № 5(10). С. 31-48. DOI: [https://doi.org/10.52058/3041-1793-2025-5\(10\)-31-48](https://doi.org/10.52058/3041-1793-2025-5(10)-31-48).
3. Harel, A. (2024). Refusal to serve in the Israel Defense Forces reserves in an era of anti-democratic judicial reform. *Critical Military Studies*, 10(4), 562-567. DOI: <https://doi.org/10.1080/23337486.2024.2324210>
4. Israel Defense Forces, Military Advocate General's Corps. (n.d.). The IDF Military Justice System. IDF. URL: <https://www.idf.il/en/mini-sites/military-advocate-generals-corps/the-idf-military-justice-system/>
5. Israel Democracy Institute. (n.d.). Military Service Law and Reserve Service Law Amendments (extension of mandatory and reserve service period): Professional Opinion. URL: <https://en.idi.org.il/articles/53409>
6. Israel Defense Forces. (2023, December 20). You received the 100th-day summon. Mitgaisim. URL: <https://www.mitgaisim.idf.il/%D7%9B%D7%AA%D7%91%D7%95%D7%AA/english/tzav-rishon/you-received-the-100th-day-summon/>
7. Top miluim.idf.il competitors & alternatives. AhrefsTop. URL: <https://ahrefstop.com/websites/miluim.idf.il/competitors>
8. Jaffe, M. (2024). Torah, War, Politics, and the Supreme Court: The 2024 Military Service of Ultra-Orthodox Yeshiva Students Bill. Talk About: Law and Religion (ICLRS). URL: <https://talkabout.iclrs.org/2024/11/18/torah-war-politics-and-the-supreme-court-the-2024-military-service-of-ultra-orthodox-yeshiva-students-bill>
9. Sokol, S. (2024). Government backs new extension to IDF reservists' service despite backlash. The Times of Israel. URL: <https://www.timesofisrael.com/government-backs-new-extension-to-idf-reservists-service-despite-backlash/>
10. Lacking Haredi manpower, IDF turns to womanpower: 1 in 5 fighters are now female (2025, May 21). Times of Israel. URL: <https://www.timesofisrael.com/lacking-haredi-manpower-idf-turns-to-womanpower-1-in-5-fighters-are-now-female/>
11. Levaton, S. (2025). Reporting back for duty: Older reservists step up in Israel's time of need. The Times of Israel. URL: <https://www.timesofisrael.com/reporting-back-for-duty-older-reservists-step-up-in-israels-time-of-need/>
12. The Government of Israel. Prime Minister Netanyahu visits Hasmonean Brigade training facility. URL: <https://www.gov.il/en/pages/event-hashmonaim150725>
13. Israel Defense Forces Strategy Document. Belfer Center for Science and International Affairs. URL: <https://www.belfercenter.org/research-analysis/israel-defense-forces-strategy-document>
14. Breuer, E. (2024). Gov't greenlights bill to extend IDF mandatory service to three years. The Jerusalem Post. URL: <https://www.jpost.com/breaking-news/article-810268>
15. Gov.il – The Government of Israel. Special Benefits. URL: <https://www.gov.il/en/pages/specialbenefits>
16. Bloch, A. (2025, May 8). Knesset c'mtee to discuss female soldiers' rights, haredi IDF integration. The Jerusalem Post. URL: <https://www.jpost.com/israel-news/article-853119>
17. Militarization, Conscription, and Superpower Politics in Israel (2025, April 30). Rosa-Luxemburg-Stiftung. URL: <https://www.rosalux.de/en/news/id/53374/militarization-conscription-and-superpower-politics-in-israel>
18. Knesset – The State of Israel. (2024, July 18). Extension of compulsory military service for men to 36 months. URL: <https://main.knesset.gov.il/en/news/pressreleases/pages/press18724r.aspx>

19. National Insurance Institute of Israel. (n.d.). Reservists – Reserve Service. National Insurance Institute. URL: <https://www.btl.gov.il/English%20Homepage/Updates-security-situation/KizbeotHB/ReserveService/Pages/MsrtimMiloeim.aspx>
20. Levush, R. (2024, January 3). Israel: Amendment Law Provides for Employment Protection for Hostages, Evacuees, Reservists, and Families Following Hamas Attack. Global Legal Monitor. Law Library of Congress. URL: <https://www.loc.gov/item/global-legal-monitor/2024-01-03/israel-amendment-law-provides-for-employment-protection-for-hostages-evacuees-reservists-and-families-following-hamas-attack/>
21. Militarization, Conscription, and Superpower Politics in Israel (2025, April 30). Rosa-Luxemburg-Stiftung. URL: <https://www.rosalux.de/en/news/id/53374/militarization-conscription-and-superpower-politics-in-israel?>
22. Institute for National Security Studies. (2025, June 5). Swords of Iron Survey Results – May 2025 [Survey]. INSS. URL: <https://www.inss.org.il/publication/survey-may-2025/>
23. Shapira, A. (2025, July 6). The State of National Resilience – Operation Rising Lion (INSS Insight No. 2004). INSS. URL: <https://www.inss.org.il/publication/rising-lion-society/>

REFERENCES:

1. Mykolaichuk, M., Petrukha, N., Akimova, L., Pozniakovska, N., Hudenko, B., & Akimov, O. (2025). Conceptual principles of analysis and forecasting threats to national security in modern conditions. *Sapienza: International Journal of Interdisciplinary Studies*, 6(2), e25029. DOI: <https://doi.org/10.51798/sijis.v6i2.985>
2. Andrusiak, M. V., Rusetskyi, R. Yu., & Akimov, O. O. (2025). *Polihraf u systemi natsionalnoi bezpeky: mizhdystsyplinarni pidkhody do pidhotovky kadriv ta zarubizhna praktyka* [Polygraph in the system of national security: interdisciplinary approaches to personnel training and foreign practice]. *Natsionalni interesy Ukrainy* [National Interests of Ukraine], (5(10)), 31–48. [https://doi.org/10.52058/3041-1793-2025-5\(10\)-31-48](https://doi.org/10.52058/3041-1793-2025-5(10)-31-48) [in Ukrainian].
3. Harel, A. (2024). Refusal to serve in the Israel Defense Forces reserves in an era of anti-democratic judicial reform. *Critical Military Studies*, 10(4), 562-567. DOI: <https://doi.org/10.1080/23337486.2024.2324210>
4. Israel Defense Forces, Military Advocate General's Corps. (n.d.). The IDF Military Justice System. IDF. URL: <https://www.idf.il/en/mini-sites/military-advocate-generals-corps/the-idf-military-justice-system/>
5. Israel Democracy Institute. (n.d.). Military Service Law and Reserve Service Law Amendments (extension of mandatory and reserve service period): Professional Opinion. URL: <https://en.idi.org.il/articles/53409>
6. Israel Defense Forces. (2023, December 20). You received the 100th-day summon. Mitgaisim. URL: <https://www.mitgaisim.idf.il/%D7%9B%D7%AA%D7%91%D7%95%D7%AA/english/tzav-rishon/you-received-the-100th-day-summon/>
7. Top miluim.idf.il competitors & alternatives. AhrefsTop. URL: <https://ahrefstop.com/websites/miluim.idf.il/competitors>
8. Jaffe, M. (2024). Torah, War, Politics, and the Supreme Court: The 2024 Military Service of Ultra-Orthodox Yeshiva Students Bill. Talk About: Law and Religion (ICLRS). URL: <https://talkabout.iclrs.org/2024/11/18/torah-war-politics-and-the-supreme-court-the-2024-military-service-of-ultra-orthodox-yeshiva-students-bill>
9. Sokol, S. (2024). Government backs new extension to IDF reservists' service despite backlash. The Times of Israel. URL: <https://www.timesofisrael.com/government-backs-new-extension-to-idf-reservists-service-despite-backlash/>
10. Lacking Haredi manpower, IDF turns to womanpower: 1 in 5 fighters are now female (2025, May 21). Times of Israel. URL: <https://www.timesofisrael.com/lacking-haredi-manpower-idf-turns-to-womanpower-1-in-5-fighters-are-now-female/>
11. Levaton, S. (2025). Reporting back for duty: Older reservists step up in Israel's time of need. The Times of Israel. URL: <https://www.timesofisrael.com/reporting-back-for-duty-older-reservists-step-up-in-israels-time-of-need/>
12. The Government of Israel. *Prime Minister Netanyahu visits Hasmonean Brigade training facility*. URL: <https://www.gov.il/en/pages/event-hashmonaim150725>
13. Israel Defense Forces Strategy Document. Belfer Center for Science and International Affairs. URL: <https://www.belfercenter.org/research-analysis/israel-defense-forces-strategy-document>
14. Breuer, E. (2024). Gov't greenlights bill to extend IDF mandatory service to three years. The Jerusalem Post. URL: <https://www.jpost.com/breaking-news/article-810268>

15. Gov.il – The Government of Israel. Special Benefits. URL: <https://www.gov.il/en/pages/specialbenefits>
16. Bloch, A. (2025, May 8). Knesset c'mtee to discuss female soldiers' rights, haredi IDF integration. The Jerusalem Post. URL: <https://www.jpost.com/israel-news/article-853119>
17. Militarization, Conscription, and Superpower Politics in Israel (2025, April 30). Rosa-Luxemburg-Stiftung. URL: <https://www.rosalux.de/en/news/id/53374/militarization-conscription-and-superpower-politics-in-israel?>
18. Knesset – The State of Israel. (2024, July 18). Extension of compulsory military service for men to 36 months. URL: <https://main.knesset.gov.il/en/news/pressreleases/pages/press18724r.aspx>
19. National Insurance Institute of Israel. (n.d.). Reservists – Reserve Service. National Insurance Institute. URL: <https://www.btl.gov.il/English%20Homepage/Updates-security-situation/KizbeotHB/ReserveService/Pages/MsrtimMiloeim.aspx>
20. Levush, R. (2024, January 3). Israel: Amendment Law Provides for Employment Protection for Hostages, Evacuees, Reservists, and Families Following Hamas Attack. Global Legal Monitor. Law Library of Congress. URL: <https://www.loc.gov/item/global-legal-monitor/2024-01-03/israel-amendment-law-provides-for-employment-protection-for-hostages-evacuees-reservists-and-families-following-hamas-attack/>
21. Militarization, Conscription, and Superpower Politics in Israel (2025, April 30). Rosa-Luxemburg-Stiftung. URL: <https://www.rosalux.de/en/news/id/53374/militarization-conscription-and-superpower-politics-in-israel?>
22. Institute for National Security Studies. (2025, June 5). Swords of Iron Survey Results – May 2025 [Survey]. INSS. URL: <https://www.inss.org.il/publication/survey-may-2025/>
23. Shapira, A. (2025, July 6). The State of National Resilience – Operation Rising Lion (INSS Insight No. 2004). INSS. URL: <https://www.inss.org.il/publication/rising-lion-society/>

S. A., DSc., prof. Akimov O.O., Zolotov A.V., Andrusiak M.V., Rusetskyi R.U.

ANALYSIS OF THE EXPERIENCE OF FORMING MILITARY LEGISLATION ON MILITARY SERVICE IN THE ISRAEL DEFENSE FORCES

Abstract. *The article presents a comprehensive analysis of Israel's experience in shaping military legislation concerning compulsory military service, with the aim of identifying its potential applicability to the reform of Ukraine's regulatory and legal framework in this domain. Based on an interdisciplinary approach incorporating methods of comparative legal analysis, normative modeling, and structural assessment of defense legislation, the study outlines the key principles of the personnel policy of the Israel Defense Forces (IDF), particularly regarding general conscription, reserve service, social compensatory mechanisms, gender integration, and judicial and parliamentary oversight. The article examines the current Israeli legal framework governing military service, including the IDF Service Law, amendments adopted in 2024-2025, judicial rulings of the Supreme Court of Israel, and Knesset decisions related to extending service terms and enhancing reserve participation. Several practical cases are synthesized, such as the establishment of specialized units for religious groups, mechanisms for income loss compensation, the implementation of digital registries of reservists' skills, and the automation of reimbursements by the National Insurance Institute. The study demonstrates the effectiveness of legal instruments aimed at maintaining mobilization resilience and ensuring the social legitimacy of military service under prolonged armed conflict. A comparative legal analysis of Ukrainian and Israeli military legislation reveals several regulatory gaps in Ukraine, including the absence of a consolidated framework law, lack of fixed service terms for mobilized personnel, an unstable system of benefits for reservists, the absence of a wartime alternative service mechanism, and the lack of an independent oversight body. Based on the analysis, the authors argue for the relevance of adapting key components of the Israeli model—such as digital platforms, social guarantees, dual parliamentary and judicial oversight, and gender integration standards. The article concludes that Israel's experience in military legislation demonstrates a high level of regulatory flexibility, operational adaptability to changing security environments, a balance between general civic duty and social compensation, and resilience amidst political challenges. The Ukrainian model can be effectively transformed through legislative unification, the implementation of strategic personnel planning, institutional consistency, and the strengthening of democratic oversight mechanisms.*

Keywords: *military legislation, military service, mobilization, reserve, social guarantees, sunset clauses, alternative service, parliamentary oversight, IDF, military justice, Ukraine, comparative analysis.*

ДІЄВА ОЦІНКА СИСТЕМИ КАДРОВОГО МЕНЕДЖМЕНТУ ЗБРОЙНИХ СИЛ УКРАЇНИ

У статті проведено поглиблений науково-теоретичний аналіз методики оцінки системи кадрового менеджменту Збройних Сил України (далі – СКМ) та визначено—перспективні напрями її удосконалення в умовах впливу динамічних змін і трансформаційних процесів, зумовлених сучасними військовими викликами та загрозами, а також з огляду на перспективи професіоналізації Збройних Сил України.

В умовах сьогодення ефективне управління людським капіталом не лише адміністративний процес, а в першу чергу визначальний чинник забезпечення боєздатності військ (сил) та в цілому національної системи стійкості.

В статті розглянуто необхідність перегляду критеріїв оцінки СКМ, які в попередні роки охоплювали лише статистично-кількісні показники, що не дозволяє сформувати цілісне уявлення про людський капітал, його якісні характеристики та потенційні спроможності, що надзвичайно важливо в умовах сучасних військових викликів та загроз.

Мета дослідження полягає у науковому обґрунтуванні необхідності розробки та запровадження методики дієвої оцінки СКМ з метою створення передумов для ефективного реагування на виникнення загроз, настання надзвичайних та кризових ситуацій усіх видів, урахуванням соціально-економічних, демографічних чинників та основоположних принципів міжнародних стандартів у сфері управління персоналом армій провідних країн світу.

Методологічну основу статті становлять системний, функціональний та порівняльний аналіз наукових публікацій вітчизняних і зарубіжних дослідників. Використано методи контент-аналізу, узагальнення, структурно-функціонального моделювання, експертного оцінювання та статистичного аналізу даних, що забезпечує комплексність та об'єктивність отриманих результатів.

Актуальність роботи полягає у визначенні критеріїв та показників дієвої оцінки СКМ, які поєднують кількісні параметри (рівень укомплектованості, плинність кадрів), якісні характеристики (професійна компетентність, морально-психологічна стійкість, лідерський потенціал) та стратегічні орієнтири (відповідність стандартам НАТО, адаптивність системи, ефективність кадрових рішень у динаміці). Запропонована концептуальна модель інтегрального індексу дозволить визначити реальний стан СКМ та виявити її слабкі місця.

Крім того, отримані в ході дослідження методика надасть можливість їх практичної апробації та використання під час реалізації Стратегії залучення, розвитку та утримання людського капіталу в силах оборони України на період до 2032 року, а також використання у процесі оцінки ефективності впровадження СКМ в системі Міноборони. Розроблена методика може бути застосовано у процесі повсякденної діяльності служб персоналу усіх рівнів, що дозволить підвищити ефективність прийняття управлінських кадрових рішень, забезпечення прозорості кадрової політики та формування професійного ядра українського війська.

Ключові слова: кадровий менеджмент, Збройні Сили України, дієва оцінка, кадрова політика, служби персоналу, військова організація, стандарти НАТО.

Вступ та постановка задачі. Система кадрового менеджменту Збройних Сил України є одним із ключових елементів забезпечення обороноздатності держави. Вона охоплює процеси планування, організації, координації та контролю, пов'язаний із залученням громадян на військову службу, їх освітою та підготовкою, супроводженням кар'єри, мотивацією, звільненням з військової служби, а також переходом від військової кар'єри до цивільного життя. Протягом тривалого часу військова кадрова політика у Збройних Сил

України (далі – ЗС України) залишалася зорієнтованою переважно на адміністративно-бюрократичні процедури, що обмежувало її гнучкість і дієвість у сучасних умовах.

Російська збройна агресія проти України, що триває з 2014 року та набула повномасштабного характеру у 2022 році, висунула нові вимоги до системи кадрового забезпечення. В умовах правового режиму воєнного стану актуалізувалася необхідність швидкого ухвалення кадрових рішень, ефективної адаптації до змінних обставин, підвищення ефективності підготовки та психологічної стресостійкості особового складу. Усе це потребує переосмислення підходів до кадрового менеджменту та запровадження дієвих механізмів його оцінки.

Нині особливого значення набуває інтеграція стандартів НАТО, які передбачають прозорість, підзвітність, орієнтацію на компетентності, розвиток лідерського потенціалу та врахування людського фактора як стратегічного ресурсу. Це вимагає формування нових критеріїв оцінки кадрового менеджменту, які виходять за межі суто кількісних показників (чисельність, плинність кадрів, рівень укомплектованості) і включають якісні характеристики — рівень мотивації, психологічну готовність, професійну гнучкість, здатність до навчання та інновацій.

Отже, проблема полягає у відсутності комплексної системи дієвої оцінки кадрового менеджменту ЗС України, яка б забезпечувала не лише констатацію наявного стану, а й дозволяла прогнозувати ефективність військової кадрової політики в динаміці та своєчасно виявляти слабкі сторони (місця).

Зв'язок із важливими науковими й практичними завданнями проявляється у наступному:

у науковій площині — у необхідності формування теоретичних моделей та методик оцінювання кадрового менеджменту ЗС України, які відповідали б сучасним стандартам військової організаційної структури;

у практичній площині — у створенні інструментів для ухвалення обґрунтованих управлінських рішень щодо комплектування, підготовки та розвитку військовослужбовців, що безпосередньо впливає на бойову готовність підрозділів і безпеку держави.

Отже, постановка проблеми визначає нагальну потребу у впровадженні дієвої системи оцінки кадрового менеджменту ЗС України, що має стати одним із дієвих елементів реалізації цілей та основних завдань, що стоять перед державою у сфері формування людського капіталу, як наряду забезпечення національної безпеки України.

Аналіз останніх досліджень і публікацій. Проблематика оцінки системи кадрового менеджменту у військових організаціях є предметом активного дослідження як в Україні, так і за кордоном. Вітчизняні та зарубіжні науковці започаткували різні напрями розв'язання цієї проблеми — від правового регулювання кадрової політики до розробки комплексних моделей управління людським капіталом (ресурсом), інтегрованих у стратегічні завдання збройних сил.

В українському науковому дискурсі особливе значення мають праці Думенка М. [1], Семененко О. [2], Попов С. [3], у яких наголошено на необхідності розробки нової системи оцінки кадрового потенціалу ЗСУ. Автори обґрунтовують, що ефективність кадрового менеджменту визначає рівень готовності військ до виконання завдань у сучасних умовах воєнних загроз. У працях Семененка О. започатковано підхід до розгляду кадрової політики як цілісної системи, тісно пов'язаної з реформуванням сектору безпеки і оборони.

Семененко О. [2] акцентує увагу на управлінні людським ресурсом у військових організаціях, де особливу роль відіграють компетентності, лідерські якості та психологічна стійкість військовослужбовців. У його роботах започатковано підхід до формування гнучкої системи оцінки, яка відображала б реальний стан кадрового забезпечення та дозволяла своєчасно ухвалювати управлінські рішення.

Попов С. [3] розглядає кадрову політику в стратегічному контексті, наголошуючи, що кадровий менеджмент має бути інтегрованою складовою оборонного планування. У працях автора закладено підхід до оцінки не лише кількісних показників (чисельність, плинність),

але й якісних індикаторів — рівень професійної підготовки, психологічна готовність, мотивація.

Проведений аналіз робіт [4] з питань правового регулювання військової кадрової політики у Збройних Силах, дає підстави стверджувати про необхідності вдосконалення нормативної бази та її наближення до євроатлантичних стандартів.

Авторами [5] зосереджена увагу на реформах кадрової політики ЗС України, обґрунтовуючи важливість оцінки процесів мобілізації, ротації та комплектування з урахуванням соціально-демографічних змін і морально-психологічного стану особового складу.

Серед зарубіжних учених значний вплив на розвиток концепцій кадрового менеджменту мають праці Г. Беккера, який визначав людський капітал головним стратегічним ресурсом організацій, та Д. Ульріха, що розробив концепцію HR як бізнес-партнера. Дж. Коттер звертав увагу на лідерство і управління змінами, що є критичним для підготовки військових командирів.

Дослідження під егідою НАТО (Allied Command Transformation, Human Capital Initiative) [6] започаткували системний підхід до оцінювання кадрових ресурсів. Ключовими критеріями визнано: якість підготовки, бойове злагодження, морально-психологічний стан, здатність особового складу до навчання та інновацій. У роботах R. Gal [7], A. Siebold [8], Ch. Taylor [9] наголошується, що морально-психологічні характеристики військовослужбовців мають визначальне значення для ефективності військової організації, тому вони повинні стати складовою оцінки кадрового менеджменту.

Отже, можна виокремити кілька напрямів, у яких започатковано розв'язання проблеми оцінки кадрового менеджменту:

Організаційно-правовий – вдосконалення нормативної бази.

Стратегічно-управлінський – інтеграція кадрової політики в систему оборонного планування.

Компетентнісний – оцінка військовослужбовців за професійними та особистісними характеристиками.

Соціально-мотиваційний – врахування морально-психологічних і соціальних факторів.

Міжнародний – формування комплексних моделей оцінювання персоналу та їх адаптація до військової сфери.

Попри значні наукові здобутки, у вітчизняній науці досі не сформовано цілісної методики дієвої оцінки системи кадрового менеджменту Збройних Сил України, яка б інтегрувала кращі практики НАТО та враховувала сучасні виклики воєнного стану. Це визначає необхідність подальших наукових досліджень.

Виділення невирішених раніше проблем. Незважаючи на велику кількість оригінальних та змістових праць як зарубіжних, так і вітчизняних вчених з досліджуваної проблематики, низка ключових аспектів досі залишається недостатньо дослідженою та практично не реалізованою у системі управління Збройних Сил України.

По-перше, наявні дослідження українських вчених зосереджуються переважно на організаційно-правових та адміністративних аспектах кадрової політики, тоді як сучасні виклики вимагають розробки комплексних моделей оцінювання, що інтегрують кількісні та якісні показники. Проблема полягає у відсутності єдиної методики, яка дозволяла б оцінювати кадровий менеджмент з позицій не лише укомплектованості та плинності кадрів, а й рівня компетентності, психологічної стійкості, лідерських якостей і мотивації військовослужбовців.

По-друге, хоча у працях [1-3] започатковані підходи до інтеграції кадрової політики в оборонне планування, але не створено системи прогнозування ефективності кадрових рішень у динаміці. Тобто бракує науково обґрунтованих індикаторів, які б дозволяли оцінювати не лише поточний стан кадрового забезпечення, а й його вплив на бойову готовність підрозділів у середній та довгостроковій перспективі.

По-третє, бракує досліджень, що враховували б умови особливого періоду та правового режиму воєнного стану. Переважна більшість наукових праць розглядає проблематику відносно мирного часу, що зумовлює їхню часткову втрату актуальності. Сучасні обставини вимагають врахування специфіки та особливостей проведення мобілізаційних заходів, психологічного виснаження та посттравматичних станів особового складу і застосування ротаційних механізмів, що в свою чергу суттєво впливає на потенційні спроможності людського капіталу ЗС України та прийняття відповідних кадрових рішень.

Отже, невирішеними залишаються такі аспекти:

відсутність єдиної комплексної методики оцінки кадрового менеджменту, яка б охоплювала весь спектр кількісних та якісних показників;

недосконалість системи прогнозування ефективності кадрових рішень у динаміці (короткій та довгостроковій перспективі) кадрового планування кар'єри військовослужбовців, у тому числі із застосуванням сучасних інформаційних технологій та програмних комплексів;

відсутність уніфікованих критеріїв (індикаторів) компетентнісної оцінки військовослужбовців, адаптованих до стандартів НАТО;

не врахування специфіки кадрового забезпечення в умовах правового режиму воєнного стану.

Таким чином, проблема дієвої оцінки системи кадрового менеджменту ЗС України досі залишається відкритою, що визначає необхідність створення нових методологічних підходів і практичних інструментів у цій сфері.

Метою зазначеної статті є: наукове обґрунтування та розробка методологічних засад дієвої оцінки системи кадрового менеджменту ЗС України, яка інтегрує кількісні, якісні показники, враховує специфіку особливого періоду та правового режиму воєнного стану а також узгоджується зі стандартами НАТО.

Виклад основного матеріалу. Система кадрового менеджменту ЗС України в сучасних умовах є одним із ключових чинників забезпечення обороноздатності держави та стійкості національної безпеки. Упродовж тривалого часу кадрова політика ЗС України будувалася на засадах адміністративно-командного управління, де головними критеріями оцінювання виступали кількісні параметри — чисельність особового складу, рівень укомплектованості, дисциплінарна практика. Такий підхід забезпечував формальний контроль і дозволяв здійснювати базовий моніторинг, проте він не враховував глибинних якісних характеристик людського капіталу ЗС України. В умовах особливого періоду та правового режиму воєнного стану подібна модель виявилася не повною мірою адаптованою до викликів, що постали перед державою та ЗС України в цілому.

Анексія Криму в 2014 році та початок бойових дій на сході України засвідчили, що існуюча система кадрового менеджменту виявилася не готовою до масової мобілізації та забезпечення якісного добору військовослужбовців. Значною проблемою стало поєднання великої кількості мобілізованих із низьким рівнем їхньої бойової підготовки, відсутністю мотиваційних механізмів і системної соціальної підтримки. Повномасштабна російська агресія 2022 року ще більше актуалізувала ці проблеми. Сучасна війна потребує від військовослужбовців не лише базової підготовки і дисципліни, а й високої професійної компетентності, лідерських навичок, здатності до швидкого прийняття рішень у стресових умовах, гнучкої адаптації до зміни ситуації.

Міжнародний досвід підтверджує, що людський капітал у військовій сфері має стратегічне значення. У збройних силах США кадровий менеджмент базується на концепції Human Capital Framework, що включає системи добору, розвитку компетентностей, оцінювання лідерського потенціалу та психологічної стійкості. В Ізраїлі акцент робиться на інтеграції бойової підготовки з психологічною підготовкою та створенні механізмів збереження кадрового ядра армії. У Польщі та країнах Балтії застосовуються системи оцінювання військовослужбовців за компетентнісними моделями, адаптованими до стандартів НАТО. Усі ці приклади свідчать: якість кадрової політики визначається не

кількістю особового складу, а його здатністю ефективно виконувати бойові завдання протягом тривалого часу.

Для ЗС України пропонується модель дієвої оцінки, яка складається з трьох взаємопов'язаних рівнів – кількісного, якісного та стратегічного.

Кількісний рівень охоплює укомплектованість, плинність кадрів, дисциплінарну статистику та базові параметри бойової підготовки.

Якісний рівень передбачає оцінювання професійних компетентностей, мотивації, морально-психологічного стану, лідерського потенціалу та потенційних спроможностей.

Стратегічний рівень орієнтується на довгострокові орієнтири розвитку ЗС України, інтеграцію стандартів НАТО та здатність кадрової системи до швидкої адаптації в умовах особливого періоду та правового режиму воєнного стану.

Для узагальнення цих показників у єдину систему використовується математичний апарат інтегральної оцінки. Інтегральний індекс ефективності системи кадрового менеджменту дозволяє об'єднати всі показники в єдиний результат, що може використовуватися як на стратегічному, оперативному так і на тактичному рівні управління. Формалізовано цей індекс визначається за сукупністю показників:

$$I_{ef} = \omega_1 \cdot I_k + \omega_2 \cdot I_{\text{я}} + \omega_3 \cdot I_c, \quad (1)$$

де I_{ef} інтегральний показник ефективності системи кадрового менеджменту;

I_k узагальнений показник кількісної оцінки (чисельні показники кадрової системи);

$I_{\text{я}}$ узагальнений показник кількісної оцінки (компетентності, мотивація, психологічна готовність);

I_c узагальнений показник стратегічної оцінки (довгострокові орієнтири, стандарти НАТО, адаптивність системи);

$\omega_1, \omega_2, \omega_3$ вагові коефіцієнти, що визначають відносну значущість кожної групи показників.

Умовою для вагових коефіцієнтів є:

$$\omega_1 + \omega_2 + \omega_3 = 1.$$

Кількісна оцінка обчислюється за виразом:

$$I_k = \frac{\sum_{i=1}^n \alpha_i \cdot K_i}{\sum_{i=1}^n \alpha_i}, \quad (2)$$

де K_i i -й кількісний показник (наприклад, укомплектованість, плинність, дисциплінарні порушення);

α_i ваговий коефіцієнт для кожного показника;

n кількість кількісних показників.

Для прикладу показника K_i може бути:

K_1 рівень укомплектованості (відношення фактичної чисельності до штатної чисельності);

K_2 плинність кадрів (частка вибулих військовослужбовців за певний період);

K_3 співвідношення офіцерського та сержантського складу (відображає баланс у структурі управління);

K_4 дисциплінарна практика (кількість порушень на 100 військовослужбовців).

Якісна оцінка обчислюється за виразом:

$$I_{\text{я}} = \frac{\sum_{j=1}^m \beta_j \cdot Q_j}{\sum_{j=1}^m \beta_j}, \quad (3)$$

де Q_j j -й якісний показник (наприклад, укомплектованість, плинність, дисциплінарні порушення);

β_j ваговий коефіцієнт для j -го показника;

m кількість якісних показників.

Для прикладу показник Q_j може бути:

Q_1 рівень професійних компетентностей (оцінюється через тести, виконання бойових нормативів, рівень підготовки);

Q_2 морально-психологічний стан (за результатами опитувань, психологічних скринінгів, рівня стресостійкості);

Q_3 мотивація військовослужбовців (готовність продовжувати службу, задоволеність умовами);

Q_4 лідерський потенціал командирів (оцінка підлеглими, рівень довіри, здатність ухвалювати рішення).

Стратегічна оцінка обчислюється за виразом:

$$I_c = \frac{\sum_{k=1}^p \gamma_k \cdot S_k}{\sum_{k=1}^p \gamma_k}, \quad (4)$$

де S_k k -й показники стратегічного рівня (відповідність стандартам НАТО, адаптивність кадрової системи, довгострокова ефективність кадрових рішень);

γ_k ваговий коефіцієнт для k -го показника;

p кількість стратегічних показників.

Для прикладу показник S_k може бути:

S_1 рівень відповідності кадрової політики стандартам НАТО (STANAG, доктрини, уніфікація процедур);

S_2 адаптивність системи (час, необхідний для заповнення критичних посад, швидкість мобілізації резервів);

S_3 ефективність кадрових рішень у динаміці (чи покращуються показники упродовж кількох ротаций/років);

S_4 здатність до міжнародної взаємодії (інтероперабельність із союзниками під час навчань і операцій).

Інтерпретація інтегрального індексу

$I_{\text{ef}} \in [0;1]$

$I_{\text{ef}} \geq 0,85$ - система кадрового менеджменту високоефективна;

$0,70 \leq I_{\text{ef}} < 0,85$ - система кадрового менеджменту ефективна, але має проблемні зони;

$0,50 \leq I_{\text{ef}} < 0,70$ - система кадрового менеджменту середньої ефективності, потребує корекційних заходів;

$I_{\text{ef}} < 0,50$ - кризовий стан системи кадрового менеджменту, потребує негайного реформування.

Практичне застосування інтегрального індексу може відбуватися на різних рівнях управління. Наприклад, командир бригади може здійснити оцінку кадрової ситуації у своєму підрозділі: кількісна оцінка відобразить ступінь укомплектованості та плинність кадрів,

якісна оцінка – рівень компетентностей та морально-психологічний стан особового складу, стратегічна – готовність бригади до інтеграції у спільні операції за стандартами НАТО. Узагальнений індекс дасть змогу визначити сильні та слабкі сторони кадрової політики й обґрунтувати потребу у додаткових ресурсах чи змінах у підготовці.

Розглянемо більш детально зазначений підхід розрахунку інтегрального індексу ефективності система кадрового менеджменту на умовній механізованій бригади у II кварталі 2025 року. На прикладі показано логіку нормування, ваги та підсумкову інтерпретацію для механізованої бригади у II кварталі 2025 року.

Вихідні дані:

Таблиця 1

K_i кількісний показник

Показник	Опис	Фактичне значення	Нормоване значення	Вага
Рівень укомплектованості	Фактична чисельність/штатна	85%	0,85	0,4
Плинність кадрів	Вибули/загальна чисельність	10%	0,90 (нормовано як 1-0,1)	0,3
Дисциплінарні порушення	На 100 в/сл	8 випадків	0,80	0,3

Таблиця 2

Q_i якісний показник

Показник	Метод оцінки	Фактичне значення	Нормоване значення	Вага
Рівень укомплектованості	% виконання нормативів	78%	0,78	0,4
Плинність кадрів	Опитування (шкала 1-5)	3,9/5	0,78	0,3
Дисциплінарні порушення	Експертна оцінка	4,2/5	0,84	0,3

Таблиця 3

S_k показники стратегічного рівня

Показник	Метод оцінки	Фактичне значення	Нормоване значення	Вага
Відповідність стандартам НАТО	Експертна шкала 0-1	0,70	0,70	0,5
Адаптивність системи (час комплектування критичних посад)	Норматив=30 діб/факт.=40	30/40=0,75	0,75	0,3
Динаміка ефективності кадрових рішень	Середній приріст КРІ за 3 роки	+5%	0,80	0,2

Порядок розрахунку інтегральних індексів:

Кількісний індекс

$$I_k = \frac{\sum_{i=1}^n \alpha_i \cdot K_i}{\sum_{i=1}^n \alpha_i}; I_k = \frac{0,4 \cdot 0,85 + 0,3 \cdot 0,90 + 0,3 \cdot 0,80}{0,4 + 0,3 + 0,3}; I_k = \frac{0,34 + 0,27 + 0,24}{1} = 0,85.$$

Якісний індекс

$$I_q = \frac{\sum_{j=1}^m \beta_j \cdot Q_j}{\sum_{j=1}^m \beta_j}; I_q = \frac{0,4 \cdot 0,78 + 0,3 \cdot 0,78 + 0,3 \cdot 0,84}{1}; I_q = 0,312 + 0,234 + 0,252 = 0,8.$$

Стратегічний індекс

$$I_c = \frac{\sum_{k=1}^p \gamma_k \cdot S_k}{\sum_{k=1}^p \gamma_k}; I_c = \frac{0,5 \cdot 0,7 + 0,3 \cdot 0,75 + 0,2 \cdot 0,80}{1}; I_c = 0,35 + 0,225 + 0,16 = 0,74.$$

Інтегральний індекс

Візьмемо вагові коефіцієнти для трьох блоків:

$\omega_1 = 0.4$ (кількісні показники важливі для бойової готовності),

$\omega_2 = 0.35$ (якісні показники — трохи менша вага, але суттєві),

$\omega_3 = 0.25$ (стратегічні показники у короткостроковій перспективі менш відчутні).

$I_{ef} = 0,4 \cdot 0,85 + 0,35 \cdot 0,8 + 0,25 \cdot 0,74;$

$I_{ef} = 0,34 + 0,28 + 0,185 = 0,805.$

Отриманий інтегральний індекс:

$I_{ef} = 0,805 (\approx 81\%).$

Це означає, що система кадрового менеджменту в умовній механізованій бригаді ЗС України є ефективною, але має простір для вдосконалення. Основні слабкі місця — це:

недостатня адаптивність (довго закриваються критичні вакансії);

неповна відповідність стандартам НАТО;

середній рівень морально-психологічної стійкості особового складу.

Наукові результати дослідження дозволяють зробити обґрунтовані висновки:

по-перше, сучасна система кадрового менеджменту ЗС України потребує переходу від одновимірних кількісних моделей до комплексних, що враховують компетентнісні, психологічні та потенційні спроможності людського капіталу;

по-друге, інтегральний індекс ефективності системи кадрового менеджменту може стати науково обґрунтованим інструментом для моніторингу, аналізу та прогнозування кадрової ситуації в Збройних Силах України;

по-третє, впровадження цієї методики створює передумови для розвитку і уніфікації складових військової кадрової політики зі стандартами, що застосовуються в арміях провідних країн НАТО.

Висновки. У результаті проведеного дослідження було встановлено, що система кадрового менеджменту ЗС України перебуває на етапі активної трансформації та модернізації, обумовленої сучасними воєнно-політичними викликами, необхідністю інтеграції до стандартів НАТО та умовами ведення широкомасштабної війни. Аналіз наукових джерел показав, що у вітчизняній і зарубіжній літературі започатковано окремі напрями вирішення проблеми, проте відсутня комплексна модель дієвої оцінки системи кадрового менеджменту, яка б охоплювала всі ключові параметри: кількісні, якісні та стратегічні.

Розроблена у статті методика інтегрує кількісні, якісні показники, враховує специфіку особливого періоду та правового режиму воєнного стану а також узгоджується зі стандартами НАТО а також дозволяє сформулювати інтегральний індекс ефективності системи кадрового менеджменту, що дає можливість оцінювати СКМ ЗС України не лише за формальними чисельними показниками, а й за рівнем компетентностей військовослужбовців, їхнім морально-психологічним станом, мотивацією, лідерським потенціалом. Запропонована методика забезпечує можливість об'єктивного моніторингу, порівняння проміжних результатів між різними підрозділами, виявлення проблемних питань та прогнозування кадрових ризиків на короткострокову, середньострокову та довгострокову перспективу.

Практична значущість отриманих результатів полягає у можливості їх використання для:

забезпечення прозорості та обґрунтованості прийняття кадрових рішень;

створення уніфікованої і ефективної системи залучення та комплектування ЗС України людським ресурсом;

формування ефективних програм підготовки персоналу, впровадження ротаційних механізмів та соціальної підтримки військовослужбовців;

створення належних умов для залучення, підготовки, розвитку і раціонального використання збереження та кадрового потенціалу ЗС України;

гармонізації системи кадрового забезпечення зі стандартами, що застосовуються в арміях провідних країн НАТО.

Водночас у ході дослідження виявлено низку проблемних питань, які потребують подальшого наукового дослідження і розв'язання:

недостатнє використання прогнозних моделей, що дозволяють оцінювати довгострокову ефективність кадрових рішень у динаміці;

нестача адаптованих до умов воєнного стану інструментарію (індикаторів) оцінювання компетентностей, внутрішнього потенціалу і професійної готовності військовослужбовців для виконання бойових завдань;

потреба в розробці гнучких алгоритмів адаптації складових кадрової політики в умовах масової мобілізації, високої ротації та психологічного виснаження особового складу;

необхідність розширення емпіричних досліджень, із урахуванням специфіки комплектування різних видів Збройних Сил України, родів військ (сил) та рівні органів військового управління.

Перспективи подальших наукових досліджень полягають у:

вдосконаленні математичного апарату інтегральної оцінки та перевірки його на практичних даних з підрозділів ЗС України;

розробці методів прогнозування кадрових потреб із використанням статистичного та імітаційного моделювання;

створенні програмного забезпечення для автоматизації обчислень інтегрального індексу та його візуалізації у вигляді інтерактивних дашбордів;

впровадженні регулярного моніторингу морально-психологічного стану особового складу та оцінки його впливу на боєздатність;

дослідженні впливу міжнародної військової співпраці та участі в миротворчих операціях на військову кадрову політику у ЗС України.

Отже, результати дослідження формують науково-методичне підґрунтя для створення ефективної оцінки системи кадрового менеджменту у ЗС України. Подальші наукові розробки мають бути спрямовані на інтеграцію теоретичних напрацювань у практику оборонного менеджменту, що сприятиме зміцненню кадрового потенціалу, підвищенню боєздатності ЗС України та наближенню України до стандартів НАТО.

ЛІТЕРАТУРА:

1. Думенко М.П. Метод оцінювання ефективності функціонування системи кадрових органів Збройних Сил України. Сучасні інформаційні технології у сфері безпеки та оборони № 1(49)/2024 С.128 – 140.

2. Семененко О., Царинник В., Баранов С., Тарасов О. Аналіз наявної системи кадрового менеджменту Збройних Сил України, її складові та елементи: структурно-функціональна модель підготовки громадян до військової служби. Military Science journal Vol 3 №1. 2025 С. 300 – 328

3. Попов С., Мельник Н., Розмазнін О., Єфіменко А. Зміст та концептуальні засади кадрового менеджменту в Збройних Силах України. Journal of Scientific Papers Social Development and Security'', 14 (1), 2024. С. 127–137.

4. Місце військового права в системі підготовки кадрів для сектору безпеки і оборони України / Перша науково-практична конференція військово-юридичного інституту Національного юридичного університету імені Ярослава Мудрого (м. Харків, 21 березня 2024 р.)

5. Stoyanova-Koval S., Popov S., Rozmaznin J., Sokur N., New concept of military personnel policy: challenges and prospects. Journal of Scientific Papers Social Development and Security'', 13 (6), 2023. С. 206–214.

6. NATO Allied Command Transformation. Human Capital Initiative. Norfolk, VA, 2015.

7. Gal R. *A Portrait of the Israeli Soldier*. – New York: Greenwood Press, 1986.
8. Siebold A. *Military Cohesion and Leadership*. – London: Routledge, 2007.
9. Taylor Ch. *Military Human Resource Management*. – Washington, 2012.

REFERENCES:

1. Dumenko, M.P. (2024). Method for evaluating the effectiveness of the functioning of the personnel system bodies of the Armed Forces of Ukraine. *Modern Information Technologies in the Sphere of Security and Defense*, № 1(49), pp. 128–140.
2. Semenenko, O., Tsarynnyk, V., Baranov, S., & Tarasov, O. (2025). Analysis of the existing personnel management system of the Armed Forces of Ukraine, its components and elements: a structural-functional model of citizens' preparation for military service. *Military Science Journal*, Vol. 3, № 1, pp. 300–328.
3. Popov, S., Melnyk, N., Rozmaznin, O., & Yefimenko, A. (2024). Content and conceptual foundations of personnel management in the Armed Forces of Ukraine. *Journal of Scientific Papers Social Development and Security*, 14(1), pp. 127–137.
4. The role of military law in the system of personnel training for the security and defense sector of Ukraine. *Proceedings of the First Scientific and Practical Conference of the Military Law Institute of Yaroslav Mudryi National Law University* (Kharkiv, March 21, 2024).
5. Stoyanova-Koval, S., Popov, S., Rozmaznin, J., & Sokur, N. (2023). New concept of military personnel policy: challenges and prospects. *Journal of Scientific Papers Social Development and Security*, 13(6), pp. 206–214.
6. NATO Allied Command Transformation. (2015). *Human Capital Initiative*. Norfolk, VA.
7. Gal, R. (1986). *A Portrait of the Israeli Soldier*. New York: Greenwood Press.
8. Siebold, A. (2007). *Military Cohesion and Leadership*. London: Routledge.
9. Taylor, Ch. (2012). *Military Human Resource Management*. Washington.

EFFECTIVE ASSESSMENT OF THE PERSONNEL MANAGEMENT SYSTEM IN THE ARMED FORCES OF UKRAINE

The article provides an extended scientific and theoretical analysis of modern approaches to the evaluation of the personnel management system of the Armed Forces of Ukraine and outlines the key directions for its improvement in the context of transformational processes caused by martial law and the transition to NATO principles and standards. The authors emphasize that effective management of personnel potential is not only an administrative task but also a strategic factor in ensuring the combat capability of military units, the resilience of the defense system, and the state's ability to withstand threats. The focus is placed on the problem of evaluating personnel policy not only by quantitative but also by qualitative and strategic parameters, which allows forming a holistic understanding of its effectiveness.

The purpose of the study is to scientifically substantiate and develop methodological foundations for an effective assessment of the personnel management system of the Armed Forces of Ukraine, taking into account new security challenges, socio-economic conditions of functioning, and international standards in the field of human resource management. The paper analyzes the international experience of NATO, the USA, Israel, and EU countries, which makes it possible to compare Ukrainian practice with the best examples of military personnel policy organization.

The methodological basis of the article consists of systemic, functional, and comparative approaches, as well as the analysis of scientific publications by domestic and foreign researchers. The methods of content analysis, generalization, structural and functional modeling, expert evaluation, and statistical data analysis are applied, which ensures the complexity and objectivity of the results obtained.

The scientific novelty of the study is determined by the formulation of criteria and indicators for the effective assessment of personnel management, which combine quantitative parameters (manning level, personnel turnover), qualitative characteristics (professional competence, moral and psychological resilience, leadership potential), and strategic guidelines (compliance with NATO standards, system adaptability, effectiveness of personnel decisions in dynamics). A conceptual model of an integral index is proposed, which makes it possible to determine the real state of personnel policy in a military organization and identify its weak points.

The practical significance of the obtained results lies in their possible direct use during the implementation of the Strategy for the Attraction, Development, and Retention of Human Capital in the Defense Forces of Ukraine until 2032, as well as in the development of programs for personnel support of the Armed Forces. The developed methodology can be applied in the activities of the Ministry of Defense, the General Staff, personnel services of operational commands, and military educational institutions. It forms the basis for improving the effectiveness of managerial decisions in the field of personnel management, ensuring transparency of personnel policy, and building the professional core of the Ukrainian Armed Forces.

Keywords: personnel management, Armed Forces of Ukraine, effective assessment, personnel policy, military organization, NATO standards.

АНАЛІЗ ПЕРСПЕКТИВНИХ МЕТОДІВ АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ ВІЙСЬКОВИХ ФАХІВЦІВ

Сортування є одним із перспективних методів аналітичної діяльності військових фахівців, який завжди використовується у разі потреби аналізу великого обсягу даних таким чином, що часто призводить до відкриття нових інсайтів. Сортування ефективне, коли елементи інформації можна розбити на категорії або підкатегорії для порівняння між собою, найчастіше з використанням програмного забезпечення для роботи з електронними таблицями. Цей метод особливо ефективний під час початкової стадії збору даних і генерації гіпотез, але він також може бути корисним під час вирішення інших завдань. У роботі відмічається, що сортування великої кількості даних у відповідні категорії, які порівнюються між собою, може надати аналітикам інформацію про тенденції схожості, відмінності або помилки розвідувальної інформації, яка інакше залишилась би непоміченою. Особливо корисно сортувати дані транзакцій, наприклад, перехоплення комунікацій або перекази товарів чи грошей. Для успішного використання сортування необхідно виконати наступні рекомендації. Переглянути категорії інформації, щоб визначити, яка категорія або комбінація категорій може показати тенденції або неправильності, що допоможе з'ясувати проблему, яка вивчається. Розмістити дані в електронній таблиці або базі даних, використовуючи стільки полів (стовпців), скільки потрібно для розрізнення між типами даних (дата, час, місце, люди, діяльність, сума тощо). Вказати кожен факт, кожен частину або гіпотезу, що стосується проблем, які важливі для вашої схеми сортування (використовуйте папір, дошку, пересувні папки або інші засоби для цього). Переглянути перелічені факти, інформацію або гіпотези в базі даних або електронній таблиці, щоб ідентифікувати ключові поля, які можуть дозволити виявити можливі закономірності або групування. Ці закономірності або групування потім ілюструють категорії схеми та можуть бути перераховані як заголовні категорії. Наприклад, якщо перевірка терористичної діяльності показує, що більшість нападів відбувається в готелях і ресторанах, але часи нападів різняться. «Місце» – головна категорія, тоді як «Дата» і «Час» – вторинні категорії. Групувати ці елементи відповідно до схеми сортування в категоріях. У подальшому в роботі будуть розглянуті методи рейтингу, оцінки та пріоритезація елементів розвідувальної інформації у будь-якому списку залежно від важливості, бажаності, пріоритету, вартості, ймовірності чи будь-якого іншого критерію.

Ключові слова: сортування, аналітична діяльність, розвідувальна інформація, типи даних, перспективні методи, рейтинг, оцінка, пріоритезація, ймовірність, критерії.

Вступ. Досвід провідних вчених аналітиків показує, що аналіз перспективних методів аналітичної діяльності військових фахівців дозволить значно підвищити її ефективність. Оскільки існує багато різних методів аналітичної діяльності, то обов'язок військових фахівців аналітиків постійно вивчати їх та вдосконалювати свої знання перспективних методів аналізу розвідувальної інформації. Неправильне використання методу сортування може приховати цінні інсайти так само легко, як і підсвітити їх. Стандартизація сортованих даних є надзвичайно важливою. Працюючи з аналітиком, який має досвід у сортуванні, ви зможете уникнути помилок у більшості випадків [1].

Коли будь-яка з перспективних методик використовується для агрегування думок групи аналітиків, ранжування, надане кожним членом групи, додається разом і усереднюється. Це означає, що думки фахівців, чиї погляди досить відмінні від інших, зливаються в середнє. В результаті, ранжування не відображає діапазон різних думок, які можуть бути присутні в групі. У деяких випадках виявлення фахівців, чиї погляди досить відмінні від інших, з меншістю думок

може мати велику цінність. Подальші дослідження можуть показати, що погляди фахівців, чий погляд досить відмінний від інших, дійсно правильні [2].

Аналіз останніх досліджень. Аналіз публікацій в області дослідження перспективних методів аналітичної діяльності, які значно підвищують її ефективність, дуже багато [1-3]. Один з найкращих прикладів досліджень, які відповідають цьому стандарту, це роботи майора-сержанта Роберта Д. Фолкера молодшого, Аналіз розвідки в центрах об'єднаної розвідки на рівні театру бойових дій: Експеримент у застосуванні структурованих методів (Вашингтон, округ Колумбія: Коледж об'єднаної військової розвідки, 2000 рік); Філіп Тетлок, Експертне політичне судження (Прінстон, Нью-Джерсі: Прінстонський університетський прес, 2005), 190–202. Ці судження були висловлені в публічних заявах і в особистих комунікаціях авторами. На думку військових вчених, шлях вирішення проблеми впровадження перспективних методів аналітичної діяльності значно покращить її якість та підвищить ефективність. У роботах: Левченко О. В., Вінник В. В., Устименко О. В. Розвідка та іноземні армії; Інформаційна робота: навчальний посібник / — Київ: «КНТ», 2022; Військовий стандарт 01.101.004. Видання 2. Воєнна розвідка. Розвідувально-інформаційна діяльність; Терміни та визначення. — К.: Міністерство оборони України, 2015; Процеси розвідувальної діяльності. Стандарт НАТО. Союзницька об'єднана настанова AJP-2.1 (видання В, варіант 1), теж розкриваються ці питання.

Мета статті. В ході проведення аналізу перспективних методів аналітичної діяльності військових фахівців виявлено, що вона складається з багатьох складових. Мета статті полягає у дослідженні їх впливу на підвищення якості аналітичної діяльності розвідників.

Виклад основного матеріалу. Протягом останніх років перспективні методи аналітичної діяльності безпосередньо впливають на підвищення ефективності аналітичної роботи при цьому особливу увагу звертають на хронології та графіки, які використовуються для організації даних про події або дії [4]. Перегляньте (або попросіть інших переглянути) відсортовані факти, інформацію або гіпотези, щоб перевірити, чи є альтернативні способи їх сортування. Вкажіть будь-яку альтернативну схему сортування для вашої проблеми. Одним із найкорисніших застосувань цієї техніки є сортування за допомогою кількох схем та аналіз результатів для виявлення кореляцій між даними та категоріями. Але пам'ятайте, що кореляція не означає причинно-наслідковий зв'язок. У якості приклада, якій підтверджує важливість оволодіння методом сортування розвідувальної інформації розглянемо випадок коли аналітики переглядають всю інформацію, що стосується програми збройних сил противника відносно зброї масового знищення (ЗМЗ). Звітність з електронної розвідки показує понад 300 000 емітерних зборів лише за минулий рік [5]. Сортування даних аналітиками за типом емітера, датами емісії та місцем показує різноманітні збільшення та зменшення активності емітерів з деякими мінорними тенденціями. Аналітики відфільтрували всі збори, окрім тих, що стосуються протиповітряної оборони. Невідфільтровану інформацію відсортовано за типом системи протиповітряної оборони, місцем та датами активності. Варто відзначити період, коли спостерігалася несподівано велике збільшення активності в системах повітряної оборони спостереження та системах раннього попередження. Аналітики переглядають відповідні зовнішні події та виявляють, що опозиційний рух за межами країни провів прес-конференцію, де деталізував ЗМЗ противника, включаючи місця активності всередині країни. Емітери систем повітряної оборони для всіх підозрілих місць активності ЗМЗ, включаючи декілька невиключених до прес-конференції, збільшилися до рівня військового спостереження протягом чотирьох годин після прес-конференції. Аналітики переглянули всі місця активності систем повітряної оборони, де спостерігалася збільшення, яке вважалося пов'язаним з прес-конференцією та програмами ЗМЗ, і виявили два місця, де спостерігалася збільшена активність, але які раніше не вказувалися як пов'язані зі ЗМЗ [6]. Ці нові місця були додані до планування збору для визначення того, який зв'язок, якщо такий є, вони мають бути пов'язані з програмою розвитку ЗМЗ. Неправильне сортування може приховати цінні інсайти так само легко, як і підсвітити їх. Стандартизація сортованих даних є надзвичайно важливою [7]. Працюючи з аналітиком, який має досвід у сортуванні,

можливо уникнути цієї пастки у більшості випадків. Сортування – це давно встановлена процедура для організації даних. Опис зроблено на основі навчальних матеріалів Агентства розвідки. Рейтинг, оцінка і пріоритезація три методики для ранжування, оцінки або пріоритезації елементів у будь-якому списку залежно від важливості, бажаності, пріоритету, вартості, ймовірності чи будь-якого іншого критерію [8]. Використання техніки ранжування часто є наступним кроком після використання техніки генерації ідей, такої як Структурований Брейнстормінг, Віртуальний Брейнстормінг або Номінальна Групова Техніка. Техніка ранжування можливо застосовувати в будь-якому випадку, коли занадто багато елементів для того, щоб їх легко ранжувати, просто переглядаючи список; ранжування має значні наслідки і його слід виконати як найточніше; або коли корисно об'єднати думки групи аналітиків. Поєднання техніки генерації ідей з технікою ранжування є відмінним способом для аналітика розпочати новий проект або забезпечити основу для співпраці в офісі або між агенціями. Техніка генерації ідей часто використовується для розробки списків таких речей, як тягучі сили, змінні, які потрібно враховувати, або важливі учасники [9]. Такі списки стають більш корисними після їх ранжування, оцінки або пріоритезації. Наприклад, ви можете визначити, які елементи є найважливішими, найкориснішими, найімовірнішими, або які потрібно виконати першими. З трьох обговорених тут методів Ранжування за допомогою голосування є найлегшим і найшвидшим у використанні, і часто цього достатньо. Однак він не є таким точним після того, як ви перейдете до верхніх двох або трьох ранжованих елементів, оскільки група, як правило, не думала так багато (і можливо, не цікавилася так сильно) про елементи, які ранжуються нижче. Ранжування за допомогою голосування також надає менше інформації, ніж Парне Порівняння або Вагове Ранжування [10]. Ранжування за допомогою голосування показує лише те, що один елемент ранжується вище або нижче за інший; воно не показує, наскільки вище або нижче. Парне Порівняння надає цю інформацію, а Вагове Ранжування надає ще більше інформації. Воно вказує критерії, які використовуються для ранжування, і надаються ваги цим критеріям для кожного елемента у списку. Під час проведення ранжування за допомогою голосування учасники групи індивідуально ранжують кожен елемент у порядку відповідно до їхнього вподобання або важливості. Залежно від кількості елементів або конкретних аналітичних потреб група може вирішити ранжувати всі елементи або лише три-п'ять. Лідер групи або фасилітатор роздає прості бюлетені, на яких перераховані всі елементи, що підлягають голосуванню. Кожен учасник голосує за своїм порядком вподобання. Якщо учасник вважає, що два елементи мають однакову вподобаність, голоси можуть бути розподілені між ними. Наприклад, якщо два елементи мають однакову вагу для другого місця, кожен з них отримує ранг 2.5. Будь-які елементи, за які не було проголосовано, вважаються зв'язаними на останньому місці. Після голосування учасників групи голоси підраховуються. Елемент з найнижчим числом отримує ранг номер один [9]. Парне порівняння порівнює кожен елемент з кожним іншим, і аналітик може присвоїти оцінку, щоб показати, наскільки важливий, бажаний або ймовірний один елемент порівняно з іншими. Ця техніка надає більше, ніж просте ранжування, оскільки вона вказує ступінь важливості або вподобання для кожного елемента [11]. Після цього список елементів може бути впорядкований за певними критеріями, такими як важливість або вподобання, за допомогою шкали типу інтервалу. У Ваговому Ранжуванні використовується визначений набір критеріїв для ранжування елементів. Аналітик створює таблицю з елементами для ранжування, переліченими у верхньому рядку, і критеріями для ранжування цих елементів, переліченими вздовж лівого краю. Є різні варіанти правильного проведення цього ранжування. Тут вибрано просту версію Вагового Ранжування для презентації, оскільки розвідувальні аналітики зазвичай роблять суб'єктивні оцінки, а не працюють з жорсткими числами. Коли будь-яка з цих методик використовується для агрегування думок групи аналітиків, ранжування, надане кожним членом групи, додається разом і усереднюється. Це означає, що думки фахівців, чий погляд досить відмінний від інших, зливаються в середнє. В результаті, ранжування не відображає діапазон різних думок, які можуть бути присутні в групі [12]. У деяких випадках виявлення фахівців, чий погляд досить відмінний від інших, з меншістю

думок можуть мати велику цінність. Подальші дослідження можуть показати, що їх думки вірні.

Висновки та напрямки подальших досліджень. Отже, в результаті аналізу перспективних методик аналітичної діяльності військових фахівців перспективні методи оцінки або пріоритезації зазвичай використовується зі структурованим Брейнстормінгом, Віртуальним Брейнстормінгом, номінальною груповою технікою та прийняття рішень – це ще один інструмент, який широко використовується для оцінки та пріоритезації ідей або варіантів. Він допомагає систематично порівнювати альтернативи на основі кількох критеріїв. З іншого боку, Метод Дельфі включає збір та синтез думок з панелі експертів для досягнення консенсусу з певного питання чи проблеми. Техніки ранжування, оцінювання та пріоритезації широко використовуються в різних галузях для аналітичних цілей. Вони пропонують структуровані підходи до оцінки та пріоритезації різних варіантів або ідей. Джерелами інформації про ці техніки є різні онлайн-платформи, такі як Вікіпедія для Ранжування за бальною системою, MindTools для Порівняння за парами та вебсайт Кембриджського університету з інженерії для Вагового ранжування. Крім того, книга Моргана Джонса «Набір інструментів мислителя» надала уявлення про процес Вагового ранжування. Хоча ці методи викладаються в деяких урядових установах, їх часто вважають складнішими, ніж це необхідно для розвідувальних застосувань, які зазвичай працюють з якісними, експертними даними, а не з кількісними метриками.

ЛІТЕРАТУРА:

1. "Ситуація бентежна": у ГУР назвали єдиний безпечний варіант для росіян в Криму. Анжеліка Байбак 17:29, 27 вересня 2023 р. https://24tv.ua/chornomorskiy-flot-sevastopoli-vibuhi-rozvidtsi-dali-poradu-rosiyanam_n2400724
2. Левченко О. В., Вінник В. В., Устименко О. В. Розвідка та іноземні армії. Інформаційна робота: навчальний посібник / — Київ: «КНТ», 2022. — 124 с.
3. bintel.org.ua/nukma/rozviduvalnij-proces-nato, 2023.
4. <https://www.nato.int/docu/review>, 2024.
5. Військовий стандарт 01.101.004. Видання 2. Воєнна розвідка. Розвідувально-інформаційна діяльність. Терміни та визначення. – К.: Міністерство оборони України, 2015. – 26 с.
6. Процеси розвідувальної діяльності. Стандарт НАТО. Союзницька об'єднана настанова АJP–2.1 (видання В, варіант 1)/ Управління стандартизації НАТО, 2016. – 80 с.
7. Сайт Принципів Прогнозування: www.forecastingprinciples.com/files/methodsselectionchart.pdf.
8. Рассел У. Френске, «Таксономия для операционных исследований», Операционные исследования 19, № 1 (январь-февраль 1971).
9. Кай Р. Т. Ларсон, «Таксономия предпосылок успеха информационных систем: исследования переменных анализа», Журнал менеджмента информационных систем 20, № 2.
10. Основи розвідувально-інформаційної діяльності: настанова Штабу розвідки Міністерства оборони Великобританії. – К.: ГУР МО України, 2015.– 51 с.
11. [/defpol.org.ua/index.php/produkty-tsentru/49-shliakh-ukrainy-do-nato/1084](https://defpol.org.ua/index.php/produkty-tsentru/49-shliakh-ukrainy-do-nato/1084), 2023.
12. Методичні рекомендації з розробки розвідувальних оцінок (за стандартами провідних країн-членів НАТО). – К.: ГУР МО України, 2018. – 118 с.

REFERENCES:

1. "The situation is embarrassing": the State Government named the only safe option for Russians in Crimea. Anzhelika Baybak 17:29, September 27, 2023 https://24tv.ua/chornomorskiy-flot-sevastopoli-vibuhi-rozvidtsi-dali-poradu-rosiyanam_n2400724
2. Levchenko O. V., Vinnyk V. V., Ustymenko O. V. Intelligence and foreign armies. Information work: study guide / — Kyiv: "KNT", 2022. — 124 p.
3. bintel.org.ua/nukma/rozviduvalnij-proces-nato/
4. <https://www.nato.int/docu/review>
5. Military standard 01.101.004. Edition 2. Military intelligence. Intelligence and information activities. Terms and definitions. - K.: Ministry of Defense of Ukraine, 2015. - 26 p.
6. Intelligence activity processes. NATO standard. Allied Joint Instruction AJP–2.1 (edition B, version 1)/

NATO Standardization Office, 2016. – 80 p.

7. Forecasting Principles website: www.forecastingprinciples.com/files/pdf/methodsselectionchart.pdf.

8. Russell W. Franske, "Taxonomy for Operational Research," Operational Research 19, No. 1 (January-February 1971).

9. Kai R. T. Larson, "Taxonomy of prerequisites for the success of information systems: research on variable analysis", Journal of Management of Information Systems 20, No. 2 (autumn 2003).

10. Basics of intelligence and information activities: instruction of the Intelligence Staff of the Ministry of Defense of Great Britain. – K.: GUR Ministry of Defense of Ukraine, 2015. – 51 p.

11. [/defpol.org.ua/index.php/produkty-tsentru/49-shliakh-ukrainy-do-nato/1084](http://defpol.org.ua/index.php/produkty-tsentru/49-shliakh-ukrainy-do-nato/1084)

12. Methodological recommendations for the development of intelligence assessments (according to the standards of leading NATO member countries). - K.: GUR Ministry of Defense of Ukraine, 2018. - 118 p.

**Ph.D. Mamich V.V., Ph.D., Maksimenko Yu.A.,
Ph.D. Didyk V.O., Buz A.V., Sherstyuk A.D.**

ANALYSIS OF PROSPECTIVE METHODS OF ANALYTICAL ACTIVITY OF MILITARY SPECIALISTS

Sorting is one of the promising methods of analytical activity of military specialists, it is always used when it is necessary to analyze a large amount of data in such a way that often leads to the discovery of new insights. Sorting is effective when items of information can be broken down into categories or sub-categories for comparison with each other, most often by a computer program such as a spreadsheet. This method is especially effective during the initial stage of data collection and hypothesis generation, but you can also be useful at other times. The work notes that sorting a large amount of data into appropriate categories, which are compared with each other, can provide analysts with information about trends, similarities, differences or irregularities of intelligence information that would otherwise go unnoticed. It is especially useful to sort transaction data, such as intercepting communications or transferring goods or money. To use sorting successfully, follow these guidelines: Review categories of information to determine which category or combination of categories may show trends or irregularities that will help you figure out the problem you are studying. Place the data in a spreadsheet or database using as many fields (columns) as you need to distinguish between data types (dates, times, places, people, activities, amounts, etc.). Specify each fact, each piece of information or hypothesis concerning the problem that is important for your sorting scheme (use paper, board, mobile folders or other means for this). Review the listed facts, information, or hypotheses in a database or spreadsheet to identify key fields that may enable the identification of possible patterns or groupings. These patterns or groupings then illustrate the schema categories and can be listed as header categories. For example, if a terrorist activity check shows that most attacks occur in hotels and restaurants, but the times of attacks vary, "Place" – the main category, while "Date" and "Time" – the secondary categories. Group these items according to the sorting scheme in categories. Further in the work will be considered methods of rating, evaluation and prioritization of elements of intelligence in any list depending on the importance, desirability, priority, cost, probability or any other criterion.

Keywords: *Sorting, analytical activity, intelligence, data types, promising methods, rating, evaluation, prioritization, probability, criteria.*

ДАНІ ПРО АВТОРІВ

Акімов Олександр Олексійович, доктор наук з державного управління, професор, Науково-методичний центр кадрової політики Міністерства оборони України, ORCID: 0000-0002-9557-2276, Scopus ID: 57218282721.

Андрусак Марк Володимирович, Департамент кадрової політики Міністерства оборони України, ORCID: 0009-0001-7708-0323.

Бобок Іван Ігорьович, доктор технічних наук, професор, професор національного університету «Одеська політехніка», ORCID: 0000-0003-4548-0709, Scopus ID: 57189374844.

Бобровнікова Кіра Юліївна, кандидат технічних наук, доцент, доцент кафедри математики та інформаційних технологій Університету економіки і підприємництва (Хмельницький), ORCID: 0000-0002-1046-893X

Буз Анатолій Вікторович, старший викладач кафедри бронетанкової техніки, Військова академія (м. Одеса), ORCID -0000-0002-2271-1861.

Василенко Євген Юрійович, старший викладач кафедри тактики Військової академії (м. Одеса), ORCID: 0009-0003-6616-8033.

Гайша Олександр Олександрович, кандидат технічних наук, доцент, науковий співробітник Інституту наук моря (Барселона, Іспанія) Institut de Ciencies del Mar CSIC, ORCID: 0000-0003-3711-547X, Scopus ID: – 55338466100.

Гайша Олена Олександрівна, виконуюча обов'язки завідувача кафедри інженерних технологій Міжнародного класичного університету імені Пилипа Орлика (м. Миколаїв), ORCID: 0009-0000-4543-912X, Scopus ID: – 57202193987.

Гурман Іван Васильович, кандидат технічних наук, доцент кафедри математики та інформаційних технологій Університету економіки і підприємництва (Хмельницький), ORCID 0000-0002-2282-3484

Дідик Валентин Олександрович, доктор філософії, доцент кафедри організації розвідувально-інформаційної роботи та технічних засобів розвідки, Військова академія (м. Одеса), ORCID: 0000-0003-4267-9122.

Єременок Сергій Володимирович, викладач кафедри тактики Військової академії (м. Одеса), ORCID: 0009-0006-5362-5313.

Ємцов Андрій Анатолійович, начальник науково-дослідного відділу військової кар'єри Науково-методичного центру кадрової політики Міністерства оборони України, ORCID: 0000-0001-7830-6542,

Зайцев Ігор Петрович, доктор філософії, доцент, начальник кафедри тактики Військової академії (м. Одеса), ORCID: 0000-0002-0619-8148.

Золотов Андрій Валерійович, ад'юнкт кафедри менеджменту персоналу і підготовки військ (сил) Національного університету оборони України, заступник начальника Науково-методичного центру кадрової політики Міністерства оборони України, ORCID: 0009-0005-6649-3877, Scopus ID: 59753433000.

Кобозєва Алла Анатоліївна, доктор технічних наук, професор, професор Одеського національного морського університету, ORCID: 0000-0001-7888-0499, Scopus ID: 57876302100.

Кольцов Руслан Юрійович, кандидат технічних наук, доцент, доцент кафедри геоінформаційних технологій Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-8441-9575.

Кондакова Анастасія Михайлівна – аспірант кафедри кібербезпеки та комп'ютерної інженерії, Київський національний університет будівництва і архітектури, Київ, ORCID: /0000-0003-1302-2244.

Кодратюк Володимир Володимирович, викладач кафедри тактики Військової академії (м. Одеса), ORCID: 0009-0009-8374-7946.

Коновалюк Микола Дмитрович, заступник начальника кафедри Військової академії (м. Одеса), ORCID: 0000-0001-7574-47155.

Князєв Сергій Миколайович, доктор філософії, старший науковий співробітник науково-дослідного відділу військової кар'єри Науково-методичного центру кадрової політики Міністерства оборони України, ORCID – 0000-0002-9746-704X.

Крилов Сергій Анатолійович, провідний науковий співробітник науково-дослідного відділу військової кар'єри Науково-методичного центру кадрової політики Міністерства оборони України, ORCID: 0009-0004-7841-5350.

Кузавков Василь Вікторович, доктор технічних наук, професор, начальник кафедри побудови

телекомунікаційних систем Військового інституту телекомунікацій та інформатизації імені Героїв Крут, ORCID: 0000-0002-0655-9759.

Кучер Анастасія Олександрівна, магістр кафедри геоінформаційних систем і технологій Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0009-0003-2360-865X.

Левінська Наталія Володимирівна, доцент кафедри геоінформаційних систем і технологій військового факультету сил підтримки та забезпечення Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-2532-2925.

Лєнков Сергій Васильович, доктор технічних наук, професор, Заслужений діяч науки і техніки України, Лауреат Державної премії України в галузі науки і техніки, головний науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0001-7689-239x, , Scopus ID: 58061035100, DBLP: 6.

Лєнков Євген Сергійович, кандидат технічних наук, старший дослідник, провідний спеціаліст міністерства енергетики України, ORCID: 0000-0001-5819-2656, Scopus ID: 57193055786.

Литвиненко Наталія Ігорівна, кандидат технічних наук, старший науковий співробітник, начальник кафедри геоінформаційних технологій Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-2203-2746.

Лоза Віталій Миколайович, кандидат технічних наук, старший дослідник, начальник відділу науково-дослідного центру Військового інституту імені Тараса Шевченка, ORCID: 0000-0002-8050-3614.

Луцишин Андрій Миколайович, доктор філософії, професор кафедри тактики Військової академії (м. Одеса), ORCID: 0000-0002-7733-7109.

Максименко Юрій Анатолійович, кандидат технічних наук, доцент, начальник кафедри організації розвідувально-інформаційної роботи та технічних засобів розвідки, Військова академія (м. Одеса), ORCID: 0000-0002-1227-2009.

Маміч Віктор Володимирович, кандидат технічних наук, доцент, доцент кафедри організації розвідувально-інформаційної роботи та технічних засобів розвідки, Військова академія (м. Одеса), ORCID: 0000-0001-5574-0901.

Міночкін Анатолій Іванович, доктор технічних наук, професор, провідний науковий співробітник науково-дослідного відділу (розвитку мереж доступу та електромагнітної сумісності) науково-дослідного управління (перспектив розвитку телекомунікаційних систем) наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут (Київ), ORCID: 0000-0002-4123-604X.

Муляр Ігор Володимирович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки Хмельницького національного університету, ORCID: 0000-0002-6659-605X.

Попов Сергій Афанасійович, кандидат технічних наук, доктор наук з державного управління, професор, професор Військової академії (м. Одеса), ORCID: 0000-0002-0729-9581.

Романенко Марія Михайлівна, доктор філософії, старший викладач кафедри побудови телекомунікаційних систем факультету телекомунікаційних мереж Військового інституту телекомунікацій та інформатизації імені Героїв Крут, ORCID: 0000-0002-0646-2797.

Русецький Руслан Юрійович, Департамент кадрової політики Міністерства оборони України, ORCID: 0009-0000-1540-0857.

Сажко Юрій Олександрович, старший викладач кафедри тактики Військової академії (м. Одеса), ORCID: 0009-0005-9912-2327.

Хлапонін Юрій Іванович, доктор технічних наук, професор, завідувач кафедри Київського національного університету будівництва і архітектури, ORCID: 0000-0002-9287-0817, Scopus ID: 57103659600.

Чорненький Віталій Іванович, кандидат технічних наук, доцент кафедри математики та інформаційних технологій Університету економіки і підприємництва (Хмельницький).

Шерстюк Андрій Дмитрович, викладач кафедри забезпечення державної безпеки Національної академії Національної гвардії України (м. Харків), ORCID: 0000-0002-7475-0467.

АЛФАВІТНИЙ ПОКАЗЧИК

Акімов О.О.	114	Крилов С.А.	126
Андрусяк М.В.	114	Кузавков В.В.	95
Бобок І.І.	68	Кучер А. О.	33
Бобровнікова К.Ю.	82	Левінська Н.В.	33,
Буз А.В.	137	Лєнков С.В.	45, 59
Василенко Є.Ю.	21	Лєнков Є.С.	59
Гайша О.О.	59	Литвиненко Н.І.	7
Гайша О.О.	59	Лоза В.М.	21
Гурман І.В.	82	Луцишин А.М.	21
Дідик В.О.	137	Максименко Ю.А.	137
Єременок С.В.	7	Маміч В.В.	137
Ємцов А.А.	126	Міночкін А.І.	95
Зайцев І.П.	7	Муляр І.В.	82
Золотов А.В.	114	Попов С.А.	45
Кобозєва А.А.	68	Романенко М.М	95
Кольцов Р.Ю.	33	Русецький Р.Ю.	114
Кондакова А.М.	103	Сажко Ю.О	7
Кондратюк В.В..	21	Хлапонін Ю.І	103
Коновалюк М.Д.	45	Чорненький В.І.	82
Князєв С.М.	126	Шерстюк А.Д.	137

РЕДАКЦІЙНА ПОЛІТИКА ТА ЕТИЧНІ НОРМИ ПРИНЦИПИ ФОРМУВАННЯ ТА ДОСТУП ДО ЗМІСТУ «ЗБІРНИКА ВІКНУ»

Редакційна політика «Збірника ВІКНУ» заснована на принципах об'єктивності та неупередженості під час відбору статей для публікації; високих вимог до якості наукових досліджень; обов'язковості та конфіденційності рецензування статей; додержання колегіальності у відборі до публікації статей; доступності та оперативності у спілкуванні з авторами; суворого дотримання авторських і суміжних прав. Запобігання протизаконним публікаціям є відповідальністю кожного автора, редактора, рецензента, видавця.

До друку приймаються оригінальні рукописи, які не були опубліковані раніше та не відправлялись до інших редакцій, які повністю відповідають вимогам стосовно оформлення та порядку подання статей.

У «Збірнику ВІКНУ» сформовані наступні рубрики: військова техніка і технології подвійного призначення, інформаційні технології, загальні питання.

Редакція підтримує політику відкритого доступу та принципи вільного поширення наукової інформації. Примірники збірників знаходяться у Національній бібліотеці України ім. В.І. Вернадського, науковій бібліотеці ім. М. Максимовича, у бібліотеці Військового інституту та інших бібліотеках України. Електронна версія розміщена на сайті інституту, на сайтах наведених бібліотек та на сайтах «Збірника ВІКНУ»: <http://miljournals.knu.ua/index.php/zbirnuk>; <http://mil.univ.kiev.ua/page/lib/31>

ЕТИКА ПУБЛІКАЦІЙ

Редакційна колегія журналу вимагає від авторів наслідувати формальним та етичним правилам підготовки і публікації наукових робіт, які вони подають до редакції журналу. Ці норми зумовлено стандартами якості наукових статей, прийнятими у світовому науковому співтоваристві, зокрема публікаційними принципами Publishing Ethics Resource Kit (PERK), рекомендаціями Elsevier, Комітету з етики публікацій (Committee on Publication Ethics, COPE), етичним кодексом вченого України, а також досвідом роботи іноземних та українських професіональних спільнот, наукових організацій, редколегій та редакцій видань.

ЕТИЧНІ ЗОБОВ'ЯЗАННЯ РЕДАКЦІЙНОЇ КОЛЕГІЇ ЖУРНАЛУ

Редакційна колегія у своїй діяльності

- керується принципами неупередженості, наукової етики рецензування, захисту інтелектуальної власності;
- несе відповідальність за рівень наукового наповнення журналу;
- виступає проти фальсифікації, плагіату, направлення автором одного рукопису до кількох журналів, багаторазового копіювання тексту статті в різних місцях, введення громадськості в оману щодо реального внеску кожного автора в опубліковану наукову роботу;
- залишає за собою право направити рукопис на розгляд сторонньому рецензенту, в тому числі ретельний відбір через «сліпе» рецензування, відхилити статтю або повернути її на доопрацювання;
- може відхилити рукопис, якщо вважає, що він не відповідає профілю журналу, чи не відповідає етиці та правилам оформлення;
- має право вилучити вже опубліковану статтю в разі виявлення порушення будь-чиїх прав або загальноприйнятих норм наукової етики, про цей факт вилучення статті редакція повідомляє як автору статті, так і організації, де було виконано дослідження та повідомляє про це у наступному номері.

Співробітники редакції не надають іншим особам інформації, пов'язаної із змістом рукописів, що перебувають на розгляді, крім осіб, які беруть участь у її фаховій оцінці.

Згідно з міжнародним законодавством щодо додержання авторського права на електронні інформаційні ресурси, матеріали сайту, електронного журналу або проєкту не можуть бути відтворені повністю або частково у будь-якій формі (електронній чи друкованій) без попередньої письмової згоди редакції журналу. Під час використання опублікованих матеріалів у контексті інших документів обов'язково необхідними є посилання на першоджерело.

ЕТИЧНІ ЗОБОВ'ЯЗАННЯ АВТОРА

Автор:

- несе відповідальність за новизну і достовірність наведених у статтях результатів, тактико-технічних та економічних показників, коректність висловлювань, а також за те, що в матеріалах не міститься інформація з обмеженим доступом;

- повинен цитувати ті публікації, які мали визначальний вплив на суть викладеного у статті, а також ті, які можуть швидко ознайомити читача з більш ранніми працями, важливими для розуміння цього дослідження, необхідно також належним чином вказувати джерела принципово важливих матеріалів, використаних у цій роботі, якщо вони не були отримані самим автором;- забезпечує недопустимість плагіату та подання до публікації раніше надрукованих матеріалів, у випадку виявлення зазначених фактів відповідальність несе автор поданих матеріалів.

Співавторами статті мають бути всі особи, що зробили вагомий науковий внесок у подану роботу і поділяють відповідальність за отримані результати. Автор, який подає рукопис до публікації, відповідає за те, щоб до списку співавторів були включені тільки ті особи, які відповідають критерію авторства, та бере на себе відповідальність за згоду інших авторів статті на її публікацію в журналі.

УВАГА!

Для авторів статей дещо доопрацьовані вимоги щодо особистих даних.

Ці дані подаються українською та англійською мовами в такій послідовності: Прізвище_Ім'я_По - батькові (за бажанням). Науковий ступінь та вчене звання. Місце роботи та посада_

ORCID 0000-0001-3215-4400

SCOPUS ID 57193059215 (за наявності) Індекс DBLP 10 (за наявності)

e-mail: __ моб. телефон_

Надсилати скановані рисунки, формули та таблиці не допускається.

Вся стаття оформлюється одним шрифтом **Times New Roman**, вказаними нижче розмірами, зверніть увагу на формули, таблиці та рисунки.

РЕДАКЦІЙНА КОЛЕГІЯ «ЗБІРНИКА ВІКНУ» ЗДІЙСНЮЄ НЕЗАЛЕЖНЕ («СЛІПЕ») ЕКСПЕРТНЕ РЕЦЕНЗУВАННЯ НАДАНИХ ДО ДРУКУ РУКОПИСІВ ТА ПЕРЕВІРКУ ЇХ НА ПЛАГІАТ. РЕЦЕНЗУВАННЯ ЗДІЙСНЮЄТЬСЯ ЗА АНОНІМНОЮ ФОРМОЮ ЯК ДЛЯ АВТОРІВ, ТАК І ДЛЯ РЕЦЕНЗЕНТІВ.

**ЯКІСНІ ПОКАЗНИКИ ЧЛЕНІВ РЕДАКЦІЙНОЇ КОМІСІЇ ПРАЦЬ ВІКНУ
НА 16.10.25 РОКУ (НА 20.03.25)**

			Scopus	Index Hirsha	DBLP
Ленков С.В.	д.т.н., проф. ВІКНУ	Lienkov Serhii	25 (21)	5 (4)	7 (6)
Анісімов А.В.	д. ф-м н., проф., член-кор. НАНУ, КНУ	Anisimov Anatoliy	121 (114)	9	40 (38)
Барабаш О.В.	д.т.н., проф. НТУУ «КПІ»	Barabash Oleg	60 (54)	20 (18)	6(5)
Гунченко Ю.О.	д.т.н., проф.ОНУ	Gunchenko Yurii	25 (23)	6	5
Жиров Г.Б.	к.т.н. с.н.с., КНУ	Zhyrov Gennadiy	14 (12)	3	3 (1)
Заславський В.А.	д.т.н., проф., КНУ	Zaslavsky Volodymyr	33 (25)	3	11 (10)
Карпінський М.П.	д.т.н., проф., УНТ Краків (Польща)	Karpinski Mikolaj	122 (111)	12 (11)	61 (51)
Лепіх Я.І.	д. ф-м н., проф.,ОНУ	Lepikh Yaroslav	59 (57)	4	0
Петров О.С.	д.т.н., проф., УНТ Краків (Польща)	Petrov Oleksandr	19	4	1
Погорілий С.Д.	д.т.н., проф., КНУ	Pogorilyy S.D.	30 (29)	8	11 (7)
Толок І.В.	к.пед. наук, доц., НУЦЗС	Tolok Igor	13 (9)	3	2
Хайрова Н.Ф.	д.т.н., проф., Umea, U(Sweden)	Khairova Nina	46 (39)	7	40 (34)
Хлапонін Ю.І.	д.т.н., проф., КНУБА	Khlaponin Yurii	38 (32)	5 (4)	21 (18)
Шаронова Н.В.	д.т.н., проф., НТУ «ХПІ»	Sharonova N.V.	29 (24)	5	31 (25)

**ПОРЯДОК ПОДАННЯ І ОФОРМЛЕННЯ СТАТЕЙ ДО "ЗБІРНИКА НАУКОВИХ
ПРАЦЬ ВІЙСЬКОВОГО ІНСТИТУТУ КІЇВСЬКОГО НАЦІОНАЛЬНОГО
УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА"**

До друку приймаються оригінальні рукописи, які не були опубліковані раніше, не були відправлені до інших редакцій та повністю відповідають вимогам щодо оформлення та порядку подання статей.

Загальні вимоги до технічного оформлення статей:

Обсяг рукопису - рекомендується **не менше 12 повних аркушів** українською або англійською мовами.

Формат аркуша - **A4 (210 x 297 мм).**

Розмір полів: верхнє, нижнє, правє, лівє - **2 см.**

Шрифт тексту - **Times New Roman №12**, через міжрядковий інтервал - **1,0**.

Абзац має становити **10 мм.**

Стаття повинна мати такі необхідні елементи:

УДК;

назва статті, яка лаконічно відображає зміст та новизну статті;

анотація та ключові слова;

вступ та постановка задачі чи проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями;

аналіз останніх досліджень і публікацій, в яких започатковано **розв'язання цієї проблеми** і на які спирається автор, визначення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття, формулювання мети статті;

виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів, практичних рішень та експериментів;

висновки з цього дослідження і перспективи подальшого розвитку в цьому напрямку,

список літератури,

References,

дані про авторів двома мовами.

Анотація до статті виконується українською та англійською мовами загальний обсяг кожної не менш ніж **1800** знаків, включаючи ключові слова.

Вона повинна містити коротке повторення структури статті, що включає вступ, цілі і завдання, методи, результати, висновки.

Анотацію друкують курсивом, шрифт Times New Roman, №11. Після анотації розміщуються **ключові слова** (5–7 термінів).

Список літератури (References) повинен включати не менш 12 джерел, з яких 50 % видані за останні 10 років. При цьому не менш 25 % джерел повинно відноситися до іноземної періодики. Самоцитування авторів у списку літератури повинно бути, як правило, не більш за 25 %.

Якщо основною мовою статті є українська, то оформляються два списки літератури: перший (список літератури мовою оригіналу джерела) – згідно з наказом МОН від 12.01.2017 № 40 та відповідно до ДСТУ 8302:2015 «Інформація та документація. Бібліографічне посилання: загальні положення та правила складання»;

другий (REFERENCES) з урахуванням ДСТУ 8302:2015, наказу МОН від 12.01.2017 № 40 та міжнародного Гарвардського стилю BSI (British Standards Institution).

На адресу редколегії (03022, м. Київ, вул. Ю. Здановської, 81, тел.: +38 (044) 521 - 33 - 82) мають бути надіслані наступні матеріали:

експертний висновок про можливість відкритого публікування, завірений печаткою, сканкопія надсилається на e-mail: lenkov_s@ukr.net

Вимоги до оформлення References

References потрібно приводити окремим блоком, повторюючи послідовність попередньо наведеного Списку літератури. Джерела при цьому оформлюються за такими основними правилами (Harvard style оформлення BSI: British Standards Institution):

– запис завжди починається з прізвища автора, потім кома, ініціали (між ініціалами пропуски не ставляться), за якими в дужках вказується дата видання; два автори відокремлюються «and» без коми; кілька авторів розділяються комами, але останнє прізвище повинно бути відокремлене «and» без коми;

– витяги з публікацій, тобто назви статей журналів, глав в книгах наводяться в "лапках";

– назва журналу або книги завжди виділяється курсивом;

– ім'я видавця вказується перед місцем видання;

– коми використовують для поділу елементів запису;

– для джерел українською або російською мовами, що наводяться у References, назви статей журналів, глави з книг наводяться латиницею (транслітерацією) в "лапках" та

перекладаються англійською мовою в квадратних дужках. Онлайн-конвертер з української мови для транслітерації: <http://translit.kh.ua/?passport>.

Приклади оформлення References за стилем Harvard British Standards Institution

Книга (ДСТУ 8302:2015)

Інформаційно-психологічна боротьба у війсьній сфері: монографія / Г.В. Певцов, А.М. Гордієнко, С.В. Залкін, С.О. Сідченко, А.О. Феклістов, К.І. Хударковський. Х.: Вид. Рожко С.Г., 2017. 276 с.

Книга (Harvard style BSI)

Pievtsov, H.V., Hordiienko, A.M., Zalkin, S.V., Sidchenko, S.O., Feklistov, A.O. and Khudarkovskyi, K.I. (2017), "Informatsiino-psykholohichna borotba u voiennoi sferi: monohrafiia" [The information and psychological struggle in the military sphere], Rozhko S.H., Kharkiv, 276 p.

Стаття із періодичного видання (ДСТУ 8302:2015)

Карпенко, Д.В. Стан та перспективи розвитку зенітного ракетного озброєння Повітряних Сил Збройних Сил України / Наука і техніка Повітряних Сил Збройних Сил України. 2017. № 2(27). С. 75–78.

Стаття із періодичного видання (Harvard style BSI)

Karpenko, D.V. (2017), "Stan ta perspektyvy rozvytku zenitnoho raketnoho ozbroiennia Povitrianykh Syl Zbroinykh Syl Ukrainy" [The state and perspectives of the development of anti-aircraft missile armaments in the Air Force of Ukraine], Science and Technology of the Air Force of Ukraine, No. 2(27), pp. 75–78.

Дисертація (ДСТУ 8302:2015)

Белозеров, І.В. Религиозная политика: дис. ... канд. ист. наук: 07.00.02; захищена 22.01.02; утв. 15.07.02 / Белозеров Иван Валентинович. К., 2002. 215 с.

Дисертація (Harvard style BSI)

Belozarov, I.V. (2002), "Relyhyoznaia polityka: dissertation" [The religious policy: dissertation], Kiev, 215 p.

Джерела електронного ресурсу віддаленого доступу (ДСТУ 8302:2015)

Романов В. К вопросу о путях достижения национальной безопасности в условиях глобализации: проблемы теории и практики в контексте внешней политики России и Польши [Електронний ресурс] Безопасность и оборона, 2016. № 1(2), С. 7–15. Режим доступа до журн.: http://www.desecuritate.uph.edu.pl/images/De_Securitate_12_2016.pdf.

Джерела електронного ресурсу віддаленого доступу (Harvard style BSI)

Romanov, V. (2016), "K voprosu o putyakh dostizheniya natsionalnoy bezopasnosti v usloviyakh globalizatsii: problemy teorii i praktiki v kontekste vneshney politiki Rossii i Polshi" [To the question about the ways to achieve national security in the context of globalization: the problems of theory and practice in the context of the foreign policy of Russia and Poland], Security and Defence Journal, No. 1(2), pp. 7–15, www.desecuritate.uph.edu.pl/images/De_Securitate_12_2016.pdf (accessed 12 July 2017). (примітка: при наведенні URL "http: //" має бути виключено).

Більш детальну інформацію щодо оформлення бібліографічних посилань за стилем Harvard British Standards Institution можна знайти на сайті **Національної бібліотеки України імені В.І. Вернадського** та онлайн генератора посилань **Cite This For Me**.

Редакційна колегія: e-mail: lenkov_s@ukr.net

Шрифт

**СХЕМА ОФОРМЛЕННЯ СТАТЕЙ
У «ЗБІРНИКУ НАУКОВИХ ПРАЦЬ ВІКНУ»**

УДК

науковий ступінь, вчене звання
ініціали та прізвище автора (співавторів)
місце роботи автора (співавторів)

12 пт

УДК 32.973.202:07.681

д.т.н., проф. Степанов С.В. (ВІКНУ)
к.т.н., с.н.с. Українець О.В. (ВІКНУ)
Саленко В.Д. (ВІКНУ)

**12 пт
жирний**

**КЕРУВАННЯ ЕЛЕКТРОННИМИ ПРИСТРОЯМИ ЗА ДОПОМОГОЮ
ЖЕСТІВ**

Анотація до статті виконується українською та англійською мовами (загальний обсяг кожної не менш, ніж **1800** знаків, включаючи ключові слова).

**11 пт
курсив,
жирний**

Для керування електронними пристроями, для сучасного користувача кльовими критеріями є такі, як: зручність та простота керування. Для того, щоб дати користувачеві такі можливості та зручності в використанні, є досить цільною розробка системи, яка б надавала такі можливості. Керування системою, яка ґрунтується на основі жестів, є надзвичайно перспективним, та може суттєво легшити користувачеві роботу з нею, тому що жести, які потрібні для керування системою, можуть бути інтуїтивно зрозумілими користувачеві, порівняно з іншими темами, які працюють за допомогою комбінацій клавіш.

Для вирішення задач керування за допомогою жестів, пропонується програмно-апаратний комплекс, який побудований на основі різних модулів, кожен з яких в свою чергу виконує відповідну роль в системі, наприклад, знаходить точку інтересу з сцени чи вираховує глибину сцени. Також у системі є ядро, яке відповідає за аналіз модифікаторів та жестів. На основі даних модулів стає можливо створити систему, яка б працювала на основі жестів. Але для створення цієї системи, потрібно вирішити певні задачі, такі як: сегментація, скелетизація, спостереження. Кожна з них містить в собі відповідні математичні моделі та визначення. Запропонований програмно-апаратний комплекс для керування природними жестами. Суть програмно-апаратного комплексу полягає в тому, щоб забезпечити користувача таким інтерфейсом, щоб він виконував роботу знаходячись частково віддалено від робочого місця, чи маніпулював інструментами на відстані, тобто за допомогою жестів. Використання запропонованого програмно-апаратного комплексу дозволить покращити умови стерильності в операційних, підвищити технічну безпеку під час виконання посередньої роботи користувача з приладами.

Ключові слова: штучний інтелект, контролери, модулі, жести, глибина сцени, точка інтересу, аналіз модифікаторів, аналіз жестів, сегментація, скелетизація, спостереження.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ СТАТТІ

12 пт **НЕОБХІДНІ ЕЛЕМЕНТИ СТАТТІ:** вступ та постановка проблеми (задачі) у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями; аналіз останніх досліджень і публікацій, в яких започатковано розв'язання цієї проблеми і на що спирається автор, виділення невирішених раніше частин загальної проблеми, яким присвячується ця стаття, формулювання цілей статті (постановка завдання), виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів; їх практичного значення та результатів експеримента чи впровадження; висновки з дослідження і перспективи подальших досліджень у цьому напрямку. **Література. References.**

УВАГА! Таблиці і рисунки друкують після посилань. Якщо у статті кілька таблиць чи рисунків - їх нумерують. Заголовки таблиць і рисунків необхідно розміщувати по центру, а нумерацію таблиць праворуч від таблиці (стиль **normal**, шрифт - **Times New Roman № 12**)

Рисунки повинні бути виконані за допомогою редактора Word, згруповані і являти собою один графічний об'єкт. Формули та позначення по тексту обов'язково набирати за допомогою Equation Editor - редактора формул Word, а не у текстовому режимі. У редакторі формул мають бути встановлені такі параметри - розміри: загальний.

12 pt. великі індекси – **10 pt** , малі індекси – **7 pt**, великі символи – **14 pt.** малі символи.

10 pt: стиль: текст, функції, змінні, матриці-вектори, числа – шрифт Times New Roman, для решти стилів – шрифт Symbol, при цьому: строк. грецькі – прямі. Великі за розміром вирази та рівняння необхідно записувати у кілька рядків.

ЛІТЕРАТУРА

Перший (список літератури на мові оригіналу джерела) – згідно з наказом МОН № 40 від 12.01.2017 та відповідно до ДСТУ 8302:2015 «Інформація та документація. Бібліографічне посилання: загальні положення та правила складання»;

другий (REFERENCES) з урахуванням ДСТУ 8302:2015, наказу МОН № 40 від 12.01.2017 та міжнародного Гарвардського стилю BSI (British Standards Institution).

ЛІТЕРАТУРА:

11 пт

ЗРАЗОК

1. Ленков С.В., Толлок І.В., Цицарєв В.М., Ленков Є.С. Моделювання процесів витрачання та поповнення ресурсу угруповання технічних об'єктів. Системи озброєння і військова техніка. Харків. 2018. Вип. 1(53). С. 155 – 162.

2. Жиров Г.Б., Ленков Є.С., Цицарєв В.М., Проценко Я.М. Моделювання процесу відмов об'єктів, що відновлюються з ієрархічною конструктивною структурою. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. Київ. 2017. Вип. 55. С. 30-39.

REFERENCES:

11 пт

ЗРАЗОК

1. Lienkov, S.V., Tolok, I.V., Tsytarev, V.N. and Lenkov, Ye.S. (2018), "Modeliuvannia protsesiv vytrachannia ta popovnennia resursu uhrupuvannia tekhnichnykh obiektiv" [Modeling of processes of expenditure and resource replenishment grouping of technical objects], Systems of Arms and Military Equipment, No. 1(53), pp. 155-162.

2. Zhyrov, G.B., Lenkov, Je.S., Cycarjev, V.M. and Procenko, Ja.M. (2017), "Modeljuvannja procesu vidmov ob'ektiv, shho vidnovljujut'sja z ierarhichnoju konstruktivnoju strukturoju" [Simulation of the process of failure of objects that are restored with a hierarchical constructive structure], Zbirnyk naukovykh prac' Vijs'kovogo instytutu Kyi'vs'kogo nacional'nogo universytetu imeni Tarasa Shevchenka, No. 55, pp. 30-39

CONTROL ELECTRONIC DEVICES USING GESTURES

For management of electronic devices, for today's user important criteria are: convenience and ease of management. In order to provide the user with such opportunities and usability to use, it is quite reasonable to develop a system that would provide such opportunities. Managing a gesture-based system is extremely promising, but can greatly facilitate the user to work with it, because the gestures that are needed to manage the system can be intuitive to the user, compared to other systems that operate using keyboard shortcuts. To solve the problems of managing using gestures, a software-hardware complex is proposed that is based on different modules, each of which in turn plays an appropriate role in the system, for example, finds a point of interest from a plurality or calculates the depth of a scene. Also, the system has a kernel that is responsible for analyzing modifiers and gestures. Based on the data of the modules it becomes possible to create a system that would work on the basis of gestures. But for the creation of this system, it is necessary to solve certain problems, such as: segmentation, skeletalization, observation. Each of them contains the corresponding mathematical models and definitions. Proposed hardware and software complex for management of natural gestures. The essence of the software and hardware complex is to provide the user with such an interface that he was performing work while being partially remote from the workplace, or manipulating tools at a distance, that is, using gestures. The use of the proposed software-hardware complex will improve the sterility parameters in the operating system, increase the technical safety during the direct work of the user with the devices.

Keywords: artificial intelligence, controllers, modules, gestures, depth of the scene, point of interest, analysis of modifiers, gesture analysis, segmentation, skeletonization, observation.

Дані про авторів див. стор.142, 143

ДЛЯ ПОДАТОК

Наукове видання



ЗБІРНИК НАУКОВИХ ПРАЦЬ

**Військового інституту
Київського національного університету імені Тараса Шевченка**

№ 88

Усі матеріали надруковані в авторській редакції

Підписано до друку 22.10.2025 р.

Авт. друк. арк. 8,00. Формат 60х90/8 Безкоштовно. Замовлення № 53-24.

Надруковано у навчальному тренувальному комплексі ВІКНУ

Київ, вул. Ю. Здановської, 81

т. 521-32-89

