

НАУКА і ОБОРОНА

Щоквартальний науково-теоретичний та науково-практичний журнал

Передплатний індекс 74303

Редакція:

Семон Богдан Йосипович (головний редактор), доктор
технічних наук, професор;

Бодрик Юрій Григорович (науковий редактор),
кандидат технічних наук, старший науковий
співробітник;

Колесник Володимир Іванович (відповідальний
секретар), кандидат технічних наук, старший
науковий співробітник

Редакційна колегія:

Бочарніков Віктор Павлович, доктор технічних наук,
професор;

Воробйов Олег Михайлович, доктор технічних наук,
професор;

Грицюк Валерій Миколайович, доктор історичних наук,
доцент;

Еггінтон Білл, доктор освіти;

Загорка Олексій Миколайович, доктор військових наук,
професор;

Карабин Василь Васильович, доктор технічних наук,
доцент;

Коваль Михайло Володимирович, доктор військових наук;

Коваль Володимир Валерійович, кандидат військових
наук, старший науковий співробітник;

Косевцов В'ячеслав Олександрович, доктор військових
наук, професор;

Лобанов Анатолій Анатолійович, доктор військових
наук, професор;

Мацько Олександр Йосипович, кандидат військових
наук, професор;

Машталір Вадим Віталійович, доктор історичних наук,
професор;

Медведев Володимир Костянтинович, кандидат
військових наук, професор;

Мірненко Володимир Іванович, доктор технічних наук,
професор;

Неділько Олександр Миколайович, кандидат технічних
наук, доцент;

Осьодло Василь Ілліч, доктор психологічних наук,
професор;

Павліковський Анатолій Казимирович, кандидат
військових наук, доцент;

Павлюк Олександр Олексійович, кандидат військових
наук;

Пунда Юрій Васильович, доктор військових наук,
старший науковий співробітник;

Ракушев Михайло Юрійович, доктор технічних наук,
старший науковий співробітник;

Руснак Іван Степанович, доктор військових наук,
професор;

Салій Анатолій Григорович, кандидат військових наук,
професор;

Самберг Андре, кандидат технічних наук;

Серватюк Василь Миколайович, доктор військових наук,
професор;

Слюсаренко Андрій Віталійович, доктор історичних
наук, професор;

Телелим Василь Максимович, доктор військових наук,
професор;

Чепков Ігор Борисович, доктор технічних наук,
професор;

Щипанський Павло Володимирович, кандидат
військових наук, професор

Зміст

Актуальні питання національної безпеки та оборони

<i>Казмірчук А. П., Савицький В. Л., Жаховський В. О., Лівінський В. Г.</i> Методологічні підходи до ресурсного забезпечення Медичних сил Збройних Сил України на засадах оборонного планування	3
<i>Слюсаренко А. В., Телелим В. М., Зельницький А. М., Заболотний О. А.</i> Забезпечення якості професійної військової освіти: визначення понять і моніторинг поточного стану	14

Розвиток теорії та методології

<i>Сафонов О. В., Семон Б. Й., Неділько О. М.</i> Метод оцінювання максимального рівня коливань аеродинамічних поверхонь керування надзвукових літаків у разі виникнення трансзвукового флатера.....	23
--	----

Національна безпека та оборона: методичний аспект

<i>Свєшніков С. В., Бочарніков В. П.</i> Використання методів штучного інтелекту для розв'язання наукових задач у сфері оборони	29
<i>Сенаторов В. М., Гурнович А. В., Мельник Б. О., Кучинський А. В.</i> Застосування стрілецької зброї для знищення дрона-камікадзе «Шахед-136»	41

Уроки російсько-української війни

<i>Mashtalir V. V., Shypovskiy V. V.</i> Analysis of the cyber domain during the Russian-Ukrainian war 2022: conclusions, recommendations, lessons learned	48
Summaries	57

Contents

Topical issues of national security and defence

<i>A. P. Kazmirchuk, V. L. Savytskyi, V. O. Zhakhovskiy, V. H. Livinskyi.</i> Methodological approaches to the resource supply of the Medical Forces of the Armed Forces of Ukraine on the basis of defence planning	3
<i>A. V. Sliusarenko, V. M. Telelym, A. M. Zelnytskyi, O. A. Zabolotnyi.</i> Quality assurance for professional military education: definition of concepts and monitoring of the current state.....	14

Розвиток теорії та методології

<i>O. V. Safronov, B. Y. Semon, O. M. Nedilko.</i> A method for estimation of the maximum level of oscillations of aerodynamic control surfaces of supersonic aircraft under transonic flutter	23
--	----

National security and defence: methodical aspect

<i>S. V. Svieschnikov, V. P. Bocharnikov.</i> Use of artificial intelligence methods for solving scientific problems in the defence area	29
<i>V. M. Senatorov, A. V. Hurnovych, B. O. Melnyk, A. V. Kuchynskiy.</i> Application of small arms to destroy the Shahed-136 kamikaze drone	41

Russia-Ukraine war: lessons learned

<i>Mashtalir V. V., Shypovskiy V. V.</i> Analysis of the cyber domain during the Russian-Ukrainian war 2022: conclusions, recommendations, lessons learned	48
Summaries	57

DOI 10.33099/2618-1614-2023-23-4-3-13

УДК 614.2:355.415.6

А. П. Казмірчук,*доктор медичних наук, професор, командувач Медичних сил Збройних Сил України, генерал-майор медичної служби,***В. Л. Савицький,***доктор медичних наук, професор, начальник Української військово-медичної академії, бригадний генерал медичної служби,***В. О. Жаховський,***кандидат наук з державного управління, доцент, провідний науковий співробітник Науково-дослідного інституту проблем військової медицини, Українська військово-медична академія,***В. Г. Лівінський,***кандидат медичних наук, провідний науковий співробітник Науково-дослідного інституту проблем військової медицини, Українська військово-медична академія*

Методологічні підходи до ресурсного забезпечення Медичних сил Збройних Сил України на засадах оборонного планування

У статті на основі аналізу діяльності Медичних сил Збройних Сил України опрацьовано та запропоновано методологічні підходи до визначення потреби в обсягах ресурсів для належного медичного забезпечення Збройних Сил України в умовах сучасних збройних конфліктів та повномасштабної збройної агресії проти України, які мають базуватися на засадах оборонного планування. Установлено, що ресурси для медичного забезпечення Збройних Сил України мають дві складові: власні ресурси Медичних сил та ресурси і послуги від системи охорони здоров'я держави та інших міністерств і відомств (економіки України). Визначено основні чинники, які мають визначальний вплив на методологію та порядок розрахунку обсягів необхідних ресурсів для медичного забезпечення Збройних Сил України.

Ключові слова: медичне забезпечення, Медичні сили Збройних Сил України, ресурси системи медичного забезпечення Збройних Сил України, оборонне планування.

© А. П. Казмірчук, В. Л. Савицький, В. О. Жаховський, В. Г. Лівінський, 2023

Постановка проблеми. Довготривала повномасштабна війна Російської Федерації проти України засвідчила важливість усебічного повноцінного ресурсного забезпечення сил оборони, у тому числі для їх медичного забезпечення. Водночас нині прорахунки в забезпеченні сил оборони вітчизняними оборонними ресурсами покриваються за рахунок міжнародної технічної допомоги та волонтерів.

Забезпечення потреб функціонування й розвитку Медичних сил Збройних Сил України (далі – Медичні сили) необхідними ресурсами (людськими, матеріальними, фінансовими тощо), на думку авторів, має бути побудоване за принципами завчасного визначення потреби в них, планування їх накопичення і зберігання, ефективного управління та оптимального використання.

Саме такі підходи покладені в основу управління медичними ресурсами у збройних силах держав – членів НАТО, зокрема в Сполучених Штатах Америки, які під час налагодження двосторонніх відносин з Медичною службою Збройних Сил України організували для керівного складу Головного військово-медичного управління Генерального штабу Збройних Сил України дворічний очно-заочний навчальний курс у рамках Міжнародної програми управління ресурсами охорони здоров'я (International Health Resources Management Program). Організатором цього навчального курсу була Військово-морська школа післядипломної освіти, Монтерей, Каліфорнія (Naval Postgraduate School, Monterey, California). Він охоплював п'ять фаз навчання, які по черзі проходили в Києві та в Сполучених Штатах Америки в органах управління медичним забезпеченням Міністерства армії США, Міністерства військово-морських сил США, Міністерства повітряних сил США, Міністерства у справах ветеранів США та в підпорядкованих їм центральних військово-медичних закладах.

У рамках навчальної програми Стратегічні ресурси інтернешнл (Strategic Resources International) військово-медичними фахівцями США був також проведений семінар «Ефективне управління» (Effective Management Seminar) з керівним складом Головного військово-медичного управління Генерального штабу Збройних Сил України.

На цей час планування розвитку ресурсів для потреб медичного забезпечення Збройних Сил України (ЗСУ) здійснюється в рамках оборонного планування шляхом визначення пріоритетів і напрямів розвитку Медичних сил, їхніх спроможностей, матеріально-технічного оснащення, інфраструктури, підготовки медичного персоналу та закладів охорони здоров'я ЗСУ, розроблення відповідних стратегій, концепцій, програм і планів, а також залучення необхідних ресурсів і послуг від системи охорони здоров'я держави та інших міністерств і відомств (економіки України) з урахуванням реальних і потенційних загроз у воєнній сфері та фінансово-економічних можливостей держави.

Метою статті є опрацювання методологічних підходів до визначення потреби в обсягах ресурсів для медичного забезпечення ЗСУ на засадах оборонного планування в умовах сучасних збройних конфліктів та повномасштабної збройної агресії проти України.

Матеріали та методи. Використані законодавчі й нормативно-правові акти України з питань оборони держави та охорони здоров'я в Україні, нормативно-правові акти й керівні документи Міністерства оборони України (МОУ) і ЗСУ з питань медичного забезпечення військ (сил) та надання медичної допомоги військовослужбовцям в умовах бойових дій.

Об'єкт дослідження – система медичного забезпечення ЗСУ. Предмет дослідження – ресурсне забезпечення потреб Медичних сил в умовах сучасних збройних конфліктів та повномасштабної збройної агресії проти України. Методи дослідження: бібліографічний, аналітичний, системного підходу, узагальнення, прогностичний.

Викладення основного матеріалу

Згідно із чинними законодавчими, нормативно-правовими актами і керівними документами оборонне планування поділяється на довгострокове, середньострокове та короткострокове [1–3].

Довгострокове оборонне планування в МОУ та ЗСУ здійснюється з метою реалізації засад державної політики у сфері оборони і військового будівництва шляхом визначення стратегічних цілей, пріоритетів і напрямів розвитку ЗСУ (сил оборони), озброєння та військової техніки, інфраструктури, підготовки військ (сил), а також потреби в ресурсах [2].

Відповідно до «Порядку організації та здійснення оборонного планування в Міністерстві оборони України, Збройних Силах України та інших складових сил оборони» [3] Командування Медичних сил ЗСУ є суб'єктом оборонного планування, а відповідно до Доктрини «Управління оборонними ресурсами» [4] – суб'єктом управління оборонними ресурсами, а отже, має завдання в межах установлених повноважень [2]:

- брати участь у проведенні аналізу воєнно-політичної, воєнно-економічної та воєнно-стратегічної обстановки, визначенні рівня реальних і потенційних загроз воєнній безпеці України;

- вносити за підпорядкованістю пропозиції щодо формування та реалізації воєнної політики;

- розробляти (за необхідності) пропозиції до Стратегії воєнної безпеки України (Воєнної доктрини), Державної програми розвитку озброєння та військової техніки, законодавчих та інших нормативно-правових актів у сфері оборони і військового будівництва;

- брати участь у розробленні ймовірних сценаріїв виникнення та розвитку кризових ситуацій, що потребують застосування сил і засобів сектору безпеки та оборони, зокрема Медичних сил ЗСУ;

- опрацьовувати концептуальні документи щодо застосування військ (сил) у перспективному безпековому середовищі;

- брати участь у формуванні пропозицій щодо визначення потреби в матеріальних, фінансових і людських ресурсах для забезпечення Медичних сил ЗСУ та Збройних Сил України загалом;

- розробляти програмні документи розвитку спроможностей Медичних сил ЗСУ, організовувати роботу в підпорядкованих закладах охорони здоров'я ЗСУ щодо виконання заходів довгострокового оборонного планування та взаємодії з іншими суб'єктами планування в частині, що їх стосується;

- замовляти у межах своїх повноважень проведення комплексних досліджень з питань довгострокового оборонного планування, прогнозування перспектив розвитку Медичних сил ЗСУ;

- брати участь в оборонному огляді, за результатами якого розробляються звіт і пропозиції до Стратегічного оборонного бюлетеня України.

Зазначені завдання знайшли своє відображення в Положенні про Командування Медичних сил Збройних Сил України [5].

Державні цільові програми на довгостроковий період розробляються з метою вирішення проблемних питань розвитку озброєння, військової та спеціальної техніки, інфраструктури й інших питань оборони. Порядок їх розроблення, затвердження і виконання визначається законодавством [2].

Таким чином, розроблена Командуванням Медичних сил і затверджена наказом Генерального штабу ЗСУ «Стратегія розвитку Медичних сил Збройних Сил України до 2035 року» [6] є складовою довгострокового планування в ЗСУ.

Середньострокове оборонне планування в МОУ та ЗСУ здійснюється з метою визначення комплексу заходів організаційного, технічного, соціального та економічного характеру, що забезпечують готовність сил оборони до виконання завдань з оборони держави, з урахуванням передбаченого законодавством щорічного бюджетного фінансування сектору оборони [2].

Середньострокове оборонне планування здійснюється на підставі положень Стратегії воєнної безпеки України, Стратегічного оборонного бюлетеня України, актів Президента України та Кабінету Міністрів з урахуванням передбаченого законодавством щорічного бюджетного фінансування сектору оборони, результатів огляду спроможностей, а також перебігу виконання програм розвитку сил оборони і відповідних державних цільових програм [2].

На середньостроковий період МОУ розробляє Стратегічну оборонну директиву з питань реалізації державної політики у сфері оборони у ЗСУ та інших складових сил оборони, а також державні цільові програми, спрямовані на розв'язання проблем у сфері оборони держави, а Генеральний штаб ЗСУ – комплексний документ з розвитку спроможностей ЗСУ [2].

Прикладом документів планування системи медичного забезпечення ЗСУ на середньостроковий період є «Концепція програми розвитку системи медичного забезпечення Збройних Сил України на період до 2020 року», затверджена наказом МОУ [7], План виконання та реалізації Воєнно-медичної доктрини України, затверджений першим заступником Міністра оборони України. На жаль, ці документи так і залишилися нереалізованими.

На цей час у рамках виконання науково-дослідної роботи «Обґрунтування шляхів розвитку системи медичного забезпечення Збройних Сил України на засадах єдиного медичного простору» («Моноліт») опрацьований проєкт Концепції розвитку Медичних сил Збройних Сил України до 2030 року.

Короткострокове оборонне планування здійснюється в МОУ та ЗСУ з метою деталізації, а в разі необхідності – уточнення показників комплексного документа розвитку спроможностей ЗСУ шляхом розроблення щорічних планів утримання та розвитку ЗСУ, вироблення раціональних управлінських рішень щодо ефективного використання наявних та виділених ресурсів [2].

На короткостроковий період щорічно розробляються:

- Військово-політичні вказівки щодо формування та реалізації воєнної політики в МОУ та ЗСУ на визначений період (наступний та два подальші за ним роки);
- спільні накази МОУ та ЗСУ з організації оборонного планування та складання проєктів кошторисів;
- накази керівників інших органів військового управління з питань оборонного планування (за потреби);
- пропозиції до попередніх показників проєкту Державного бюджету України на наступний рік, прогнозу видатків на два подальші роки (на перспективу – пропозиції до бюджетної декларації на три роки) та змін до переліку бюджетних програм;
- бюджетний запит МОУ;
- пропозиції МОУ до проєкту основних показників державного оборонного замовлення на відповідний період;
- зведений кошторис МОУ;
- орієнтовний план утримання та розвитку ЗСУ;
- план утримання та розвитку ЗСУ;
- план утримання та розвитку видів ЗСУ.

За потреби можуть розроблятися інші документи, які деталізують та обґрунтовують необхідність проведення заходів і витрат на них. Процес короткострокового оборонного планування здійснюється циклічно й узгоджується з бюджетним процесом в Україні [2].

Звичайно Командування Медичних сил у межах установлених повноважень бере участь у напрацюванні вказаних документів в інтересах розвитку Медичних сил ЗСУ.

Відповідно до «Рекомендацій з оборонного планування на основі спроможностей в Міністерстві оборони України та Збройних Силах України» [2], «Порядку організації та здійснення оборонного планування в Міністерстві оборони України, Збройних Силах України та інших складових сил оборони» [3], Доктрини «Управління

оборонними ресурсами» [4] та «Рекомендацій з порядку організації проведення оцінювання спроможностей у Збройних Силах України» [8] оборонне планування в МОУ та ЗСУ здійснюється із застосуванням методу планування на основі спроможностей, що передбачає розвиток спроможностей сил оборони в умовах протидії загрозам та ризикам на довгострокову перспективу в межах наявних ресурсів.

Таким чином, оборонне планування на основі спроможностей передбачає здійснення аналізу завдань та функцій Медичних сил у ймовірних варіантах застосування ЗСУ, що трансформуються у вимоги до їхніх спроможностей, на підставі чого планується їх створення, утримання та розвиток. Як результат передбачається створення, розвиток і підтримання оптимального складу необхідних спроможностей Медичних сил ЗСУ в межах наявних ресурсів [9].

Водночас слід зазначити, що матеріальні ресурси не завжди є визначальним фактором розвитку спроможностей. Ефективними шляхами їх нарощування є також удосконалення нормативно-правової та доктринальної бази медичного забезпечення військ (сил), формування структур органів управління медичним забезпеченням, закладів охорони здоров'я ЗСУ, впровадження нових організаційних засад, методів і методик надання медичної допомоги, покращення системи відбору, навчання, підготовки, перепідготовки та мотивації медичного персоналу тощо [9].

Застосування такого підходу, за яким оборонне планування в МОУ та ЗСУ здійснюється з урахуванням передбаченого законодавством щорічного бюджетного фінансування сектору оборони та в межах наявних ресурсів, є дещо нелогічним. На думку авторів, оборонне планування як основа розвитку й досягнення необхідних спроможностей у забезпечення обороноздатності держави має бути основою для бюджетного фінансування сектору оборони і визначення для цього обсягу та переліку необхідних ресурсів. У разі неможливості досягнення необхідних спроможностей і накопичення відповідних оборонних ресурсів в умовах недостатнього фінансування під час короткострокового або середньострокового планування ці показники мають бути скориговані в довгостроковому оборонному плануванні та досягатися шляхом розроблення й реалізації державних цільових програм.

Детально порядок планування розвитку системи медичного забезпечення ЗСУ авторами наведений у статті «Планування на основі спроможностей: нова парадигма розвитку Медичних сил Збройних Сил України» [9].

Для планування розвитку спроможностей Медичних сил основними вихідними даними є розрахунок їхньої потреби в необхідних людських, матеріальних, фінансових та інших ресурсах. На думку авторів, визначення потреби в необхідних ресурсах для медичного забезпечення ЗСУ та розрахунок їхньої кількості має проводитися за таким алгоритмом (рис. 1).

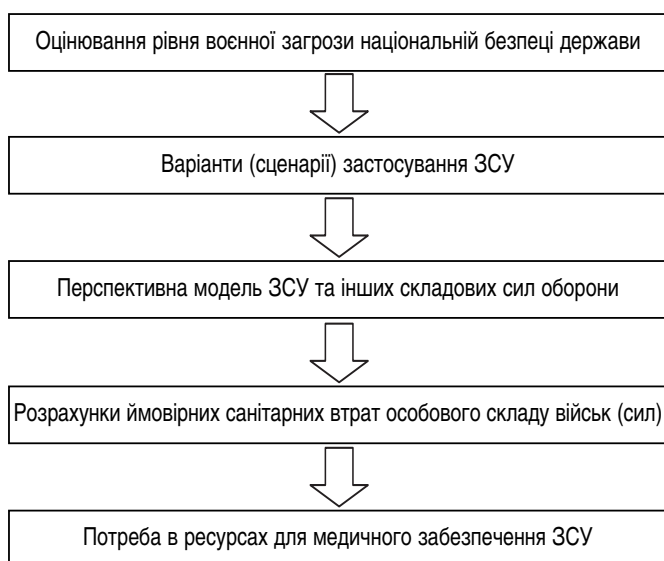


Рис. 1. Алгоритм визначення потреби в необхідних ресурсах для медичного забезпечення ЗСУ

При цьому береться до уваги, що:

- оцінка рівня воєнної загрози національній безпеці держави визначається Стратегією національної безпеки України [10];
- імовірні варіанти (сценарії) застосування сил оборони, перспективна модель ЗСУ та інших складових сил оборони визначаються Стратегією воєнної безпеки України [11];
- розрахунки ймовірних санітарних втрат особового складу військ (сил) проводяться Командуванням Медичних сил та іншими органами управління медичним забезпеченням військ (сил) спільно з органами управління персоналом у ЗСУ відповідно до методик, затверджених Генеральним штабом Збройних Сил України [12, 13] та Довідника оперативно-тактичних розрахунків з медичного забезпечення Збройних Сил України [14];
- потреба в ресурсах для медичного забезпечення ЗСУ розраховується безпосередньо Командуванням Медичних сил.

З огляду на досвід медичного забезпечення ЗСУ та інших складових сил оборони під час відбиття повномасштабної збройної агресії РФ проти України ресурси для медичного забезпечення ЗСУ мають дві складові: власні ресурси Медичних сил Збройних Сил України та ресурси й послуги від системи охорони здоров'я держави та інших міністерств і відомств (економіки України).

Власні ресурси Медичних сил включають необхідну законодавчу та нормативно-правову базу системи військової охорони здоров'я та надання медичної допомоги військовослужбовцям; розраховану мінімально необхідну кількість медичного персоналу та закладів охорони здоров'я, евакуаційно-транспортних частин і підрозділів у складі ЗСУ; забезпечення їх медичним майном, комп-

лектно-табельним оснащенням, спеціальною медичною технікою та евакуаційно-транспортними засобами, необхідною інфраструктурою для використання як у стаціонарних, так і в польових умовах; сучасні технології надання медичної допомоги військовослужбовцям у мирний час та в особливий період (рис. 2).

За досвідом медичного забезпечення ЗСУ та інших складових сил оборони під час відбиття повномасштабної збройної агресії РФ проти України власних ресурсів Медичних сил недостатньо для забезпечення надання медичної допомоги пораненим, ураженим, травмованим і хворим військовослужбовцям ЗСУ та інших складових сил оборони. У передбаченні цього постановою Кабінету Міністрів України «Про затвердження мобілізаційних завдань (замовлень) на особливий період» [15] були визначені перелік та обсяги послуг і матеріальних засобів, які передаються ЗСУ та іншим складовим сил оборони для медичного забезпечення військ (сил) в умовах бойових дій під час відбиття повномасштабної збройної агресії проти України. Крім того, порядок надання цих послуг та їхні кількісні показники були регламентовані й деталізовані в постанові Кабінету Міністрів України «Про затвердження Воєнно-медичної доктрини України» [16], розпорядженні Кабінету Міністрів України «Деякі питання медичного забезпечення військовослужбовців, осіб рядового і начальницького складу та поліцейських, які беруть участь в антитерористичній операції та здійсненні заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації у Донецькій та Луганській областях» [17] та спільному наказі МОУ та Міністерства охорони здоров'я (МОЗ) України «Про визначення механізму надання вторинної (спеціалізованої) і третинної (високоспеціалізованої) медичної допомоги військовослужбовцям, які беруть участь в антитерористичній операції та здійсненні заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації та/або в умовах запровадження воєнного чи надзвичайного стану» [18].

Основою для проведення розрахунків з метою визначення потреби в необхідних ресурсах для медичного забезпечення ЗСУ (рис. 3) є:

- варіанти (сценарії) застосування ЗСУ;
- чисельність і структура ЗСУ;
- показники санітарних втрат особового складу військ (сил) в операціях (бойових діях);
- установлені часові нормативи (показники) надання медичної (домедичної) допомоги на передових рівнях медичного забезпечення;
- нормативні показники часу для надання медичної допомоги пораненим, ураженим, травмованим і хворим військовослужбовцям на першому-другому рівнях медичного забезпечення і тривалість їхнього лікування на третьому-четвертому рівнях медичного забезпечення;
- нормативи забезпечення медичних підрозділів військових частин (з'єднань), військово-медичних

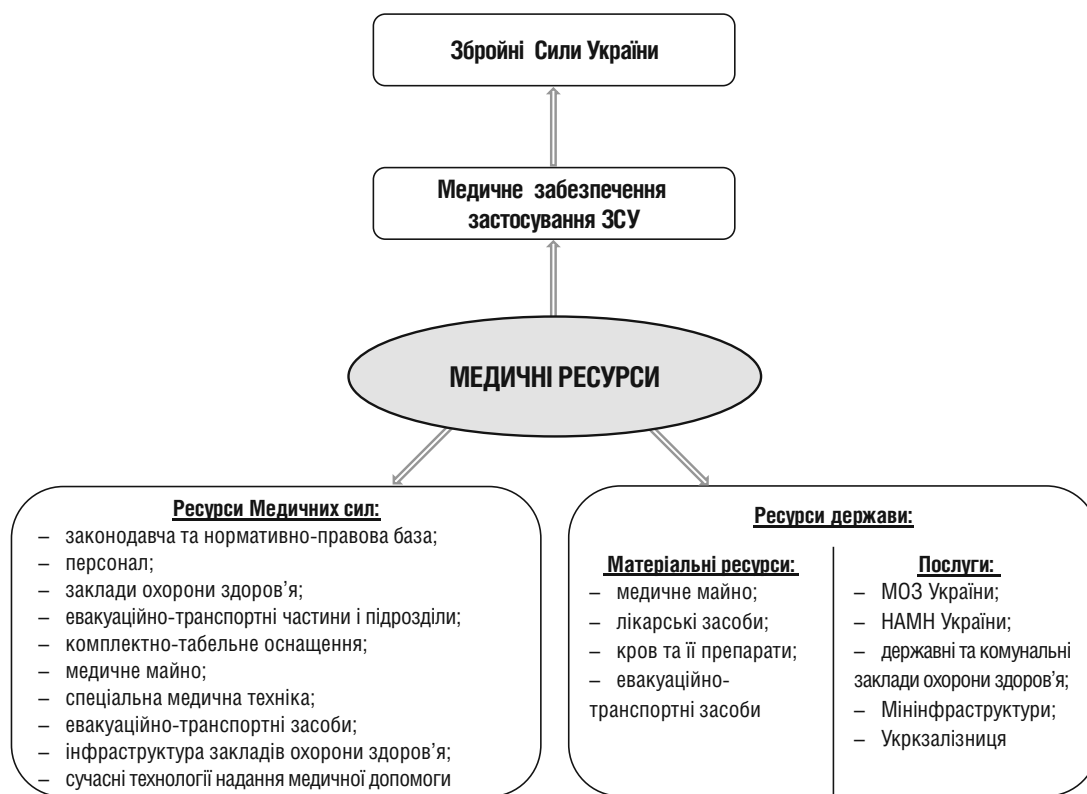


Рис. 2. Структура необхідних ресурсів для медичного забезпечення ЗСУ

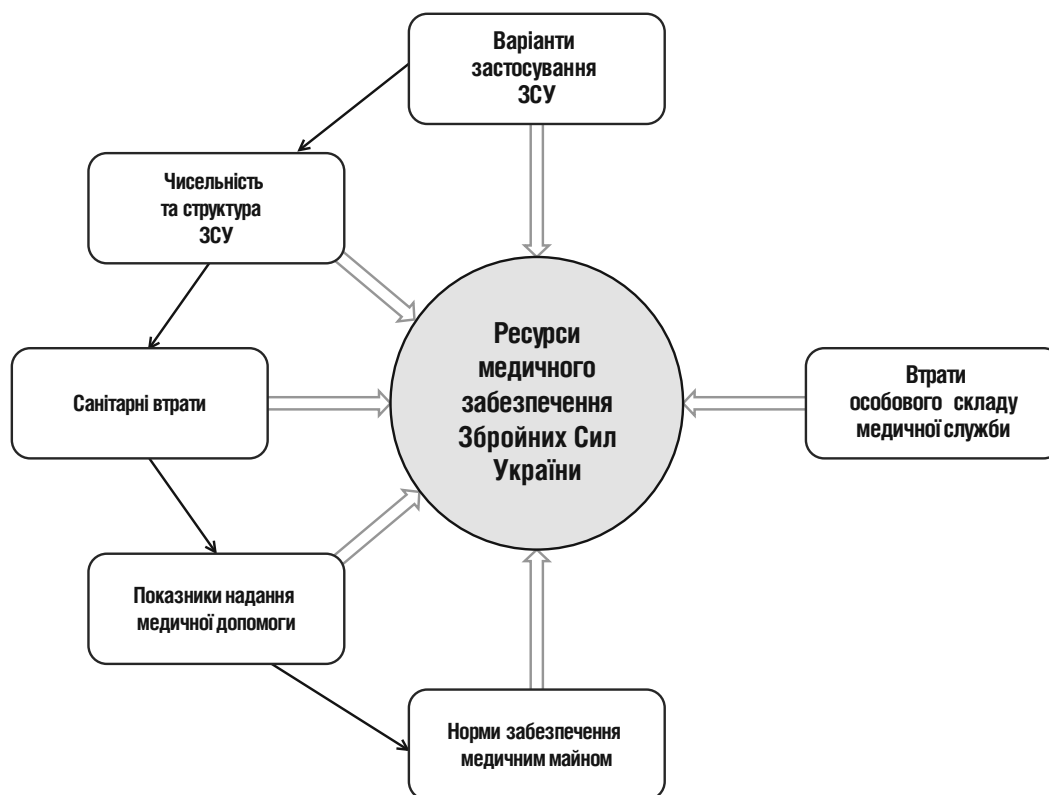


Рис. 3. Чинники, що впливають на розрахунок переліку та обсягу ресурсів для медичного забезпечення ЗСУ

закладів, санітарно-транспортних частин і підрозділів медичним майном та санітарно-технічним обладнанням для надання медичної допомоги, а також санітарно-транспортними засобами для медичної евакуації;

- показники загальних (безповоротних і тимчасових) втрат особового складу медичної служби в особливий період;

- показники втрат медичного майна та санітарно-транспортних засобів в особливий період.

Показники санітарних втрат особового складу військ (сил), а також принципи своєчасності, послідовності і преемственності під час надання медичної допомоги пораненим, ураженим, травмованим і хворим військово-службовцям є основними та визначальними чинниками в розрахунку обсягу необхідних ресурсів для медичного забезпечення ЗСУ.

Основним ресурсом у системі медичного забезпечення ЗСУ є медичний персонал. Методичними підходами та основними критеріями для визначення потреб у медичному персоналі для ЗСУ є:

- чисельність і структура ЗСУ;
- організаційно-штатна структура медичних підрозділів військових частин (з'єднань), розрахована для забезпечення надання повного обсягу встановлених видів медичної допомоги;
- організаційно-штатна структура військово-медичних закладів (військово-медичних центрів, військових стаціонарних і мобільних госпіталів тощо) та їх необхідна кількість для забезпечення надання в повному обсязі встановлених видів та обсягів медичної допомоги;
- кількість медичного персоналу для підсилення нижчих рівнів медичного забезпечення;
- показники загальних (безповоротних і тимчасових) втрат особового складу медичної служби в особливий період.

Імовірні сценарії застосування сил безпеки та оборони для виконання завдань з оборони України з розподілом відповідальності складових сектору безпеки та оборони за організацію оборони України, захист її суверенітету, територіальної цілісності й недоторканності визначені «Стратегією воєнної безпеки України» [11], а чисельність і структура ЗСУ затверджуються Верховною Радою України за поданням Президента України [19].

Розрахунки санітарних втрат на рівні військових підрозділів, військових частин (з'єднань) та угруповань військ (сил) ЗСУ в різних сценаріях їх застосування проводяться відповідно до порядку, викладеного в Довіднику оперативно-тактичних розрахунків з медичного забезпечення Збройних Сил України [14] та відповідних методик, затверджених Генеральним штабом Збройних Сил України [12, 13].

Розрахунки організаційно-штатної структури медичних підрозділів військових частин (з'єднань) та військово-медичних закладів проводяться відповідно до показників, установлених Довідником оперативно-тактичних розрахунків з медичного забезпечення Збройних Сил України [14].

З урахуванням визначеної потреби в необхідній кількості медичного персоналу (беручи до уваги показники загальних (безповоротних і тимчасових) втрат особового складу медичної служби в особливий період) формується система військово-медичної освіти й визначається порядок професійної підготовки медичного персоналу.

Особовий склад Медичних сил у ЗСУ представлений:

- військовослужбовцями, які не мають медичної освіти, водночас пройшли підготовку з надання першої медичної (домедичної) допомоги: стрільцями-санітарами, бойовими та старшими бойовими медиками, екіпажами евакуаційних підрозділів, санітарними інструкторами;
- військовослужбовцями та працівниками ЗСУ (молодшими спеціалістами), які закінчили медичні вищі навчальні заклади освіти I рівня акредитації (училища, технікуми) та одержали неповну вищу медичну освіту, а також бакалаврами, які одержали базову вищу медичну освіту у вищих закладах освіти II рівня акредитації (коледжах): медичними сестрами, операційними сестрами, сестрами-анестезистками, фельдшерами, клінічними та рентген-лаборантами та ін.;
- військовослужбовцями та працівниками ЗСУ – лікарями і провізорами.

Підготовка стрільців-санітарів, бойових і старших бойових медиків проводиться відповідно до затверджених навчальних програм у навчальних центрах (школах) ЗСУ, а її обсяг має забезпечувати повну укомплектованість військових частин (з'єднань), а також поповнення безповоротних і тимчасових втрат особового складу медичної служби в особливий період.

Підготовка медичних сестер, операційних сестер, сестер-анестезисток, фельдшерів, клінічних та рентген-лаборантів здійснюється в цивільних навчальних закладах системи охорони здоров'я України, а комплектування медичних підрозділів військових частин (з'єднань) та військово-медичних закладів здійснюється шляхом прийому на військову службу або під час мобілізації чи укладення трудового договору.

З метою належної підготовки, а в подальшому ефективного використання молодших та середніх медичних працівників у медичних підрозділах військових частин (з'єднань) та військово-медичних закладах вони під час навчання мають проходити обов'язкову підготовку з військової медицини, яка має забезпечити їхню ефективну професійну діяльність під час надання медичної допомоги пораненим, ураженим, травмованим і хворим військово-службовцям у мирний час та в умовах бойових дій.

Підготовка військових лікарів і провізорів для потреб ЗСУ та інших військових формувань здійснюється в Українській військово-медичній академії. Обсяги такої підготовки (щорічне державне замовлення) мають забезпечувати повне укомплектування медичних підрозділів військових частин (з'єднань) та військово-медичних закладів у лікарях і провізорах. Водночас в умовах мобілізаційного розгортання ЗСУ та під час тривалих збройних конфліктів виникає необхідність у прийнятті

на військову службу (мобілізації) значної кількості лікарів і провізорів із системи цивільної охорони здоров'я. При цьому в непоодиноких випадках виникає правова колізія: ці лікарі та провізори не мають відповідної підготовки з військової медицини, не мають військового звання офіцера запасу та приймаються/призиваються на військову службу на посади рядового чи сержантського складу, призначаються на посади бойових медиків, і такі випадки непоодинокі.

Усе це є наслідком того, що в певний період реформування й розвитку ЗСУ були скорочені кафедри екстремальної та військової медицини в більшості вищих медичних навчальних закладів, а підготовка офіцерів медичної служби запасу стала лімітованою в межах замовлення та за кошти фізичних і юридичних осіб, тобто платною. Наслідком такого «розвитку» стала ще одна колізія – щоб захищати свою батьківщину на посаді військового лікаря громадянину України необхідно спочатку заплатити гроші за отримання військового звання офіцера медичної служби запасу.

Який же вихід? На думку та переконання авторів, є два варіанти розв'язання цієї проблеми:

- перший – радикальний – відновлення підготовки офіцерів медичної служби запасу як базової (нормативної) складової змісту вищої медичної освіти. До речі, Міністерство освіти і науки України анонсувало, що з вересня 2024 р. у вищих навчальних закладах України з'являться військові кафедри, базова військова підготовка стане обов'язковою для всіх юнаків, а дівчата проходилимуть її за бажанням, про що проінформував суспільство заступник міністра зазначеного Міністерства [20];

- другий – безумовне виконання вимог підпункту 3 пункту 51 (зі змінами) «Положення про проходження громадянами України військової служби у Збройних Силах України» [21], затвердженого Президентом України на виконання вимог Закону України «Про військовий обов'язок і військову службу» [22]. Цим Указом встановлено, що військове звання молодшого лейтенанта запасу присвоюється «військовозобов'язаним, які не проходили військову службу, і жінкам, якщо вони мають вищу освіту ступеня магістра або прирівняний до нього освітньо-кваліфікаційний рівень спеціаліста (повна вища освіта) за спеціальністю, спорідненою з відповідною військово-обліковою спеціальністю, за результатами атестування осіб до офіцерського складу, які перебувають у запасі, з урахуванням потреби в офіцерах такої спеціальності, за переліком військово-облікових спеціальностей, який визначається Міністерством оборони України». Отже, призов/прийняття лікарів та провізорів на посади осіб рядового та сержантського складу є порушенням вимог Указу Президента України та невиконанням положень зазначеного Закону України.

На цей час Командування Медичних сил ЗСУ власними зусиллями через Українську військово-медичну академію проводить допідготовку цих лікарів з військової медицини, що дає можливість атестувати їх до присвоєн-

ня військового звання офіцера медичної служби. Водночас щоб уникнути таких проблем у майбутньому необхідно забезпечити жорсткий контроль за дотриманням територіальними центрами комплектування і соціальної підтримки вимог «Положення про проходження громадянами України військової служби у Збройних Силах України» під час прийняття на військову службу лікарів та провізорів [21].

Наступними важливими чинниками, що впливають на розрахунок переліку та обсягів ресурсів для медичного забезпечення ЗСУ, є:

- часові показники (нормативи) надання медичної допомоги на передових рівнях медичного забезпечення, встановлені «Настановою з медичного забезпечення Збройних Сил України на особливий період» [23], а саме 10 – 1 – 2, що означає: надання домедичної допомоги не пізніше 10 хвилин від моменту поранення, ураження або травми; надання першої лікарської допомоги упродовж однієї години від моменту поранення; проведення невідкладних заходів кваліфікованої медичної допомоги протягом однієї та не пізніше двох годин з моменту поранення;
- нормативні показники часу надання медичної допомоги пораненим, ураженим, травмованим і хворим військовослужбовцям на першому-другому рівнях медичного забезпечення і тривалість їхнього лікування на третьому-четвертому рівнях медичного забезпечення, визначені Довідником оперативного-тактичних розрахунків з медичного забезпечення Збройних Сил України [14].

При цьому беруться до уваги такі показники:

- потреба (у відсотках) у наданні певних видів та обсягів медичної допомоги на кожному рівні медичного забезпечення;
- час її надання медичним персоналом відповідного рівня кваліфікації;
- тривалість перебування (надання медичної допомоги та лікування) поранених, уражених, травмованих і хворих на кожному рівні медичного забезпечення;
- частка поранених, уражених, травмованих і хворих, які залишаються на кожному рівні медичного забезпечення та підлягають евакуації на вищі рівні медичного забезпечення;
- частка поранених, уражених, травмованих і хворих військовослужбовців, які потребують тривалої медичної та медико-психологічної реабілітації в стаціонарних умовах у центрах медичної реабілітації та санаторно-курортного лікування або в реабілітаційних госпіталях ЗСУ.

Ці показники (нормативи) беруться за основу під час проведення розрахунків організаційно-штатної структури медичних підрозділів військових частин (з'єднань), структури та кількості військово-медичних закладів, санітарно-транспортних частин і підрозділів, потреби в медичному персоналі, медичному та санітарно-технічному майні, кількості й видах (типах) санітарно-транспортних засобів.

Для проведення розрахунків потреби в ресурсах для медичного забезпечення ЗСУ береться до уваги, що

медичне забезпечення ЗСУ на першому та другому рівнях медичного забезпечення здійснюється за рахунок власних ресурсів Медичних сил. Водночас із урахуванням досвіду медичного забезпечення ЗСУ під час відбиття повномасштабної збройної агресії РФ проти України автори вважають за необхідне запропонувати варіант розрахунку потреби ЗСУ в ресурсах для надання спеціалізованої медичної допомоги на третьому та четвертому рівнях медичного забезпечення, а саме потреби в кількості стаціонарних ліжок для надання медичної допомоги пораненим, ураженим, травмованим і хворим військово-службовцям у цивільних закладах охорони здоров'я.

Таку потребу можна розрахувати за формулою:

$$A = \frac{B \times C \times D}{E},$$

де A – потреба в ліжковому фонді;

B – щодобові санітарні втрати (поранені, уражені, травмовані та хворі);

C – коефіцієнт потреби в щодобовій госпіталізації поранених, уражених, травмованих та хворих військово-службовців;

D – кількість прогнозованих діб воєнного конфлікту;

E – оборот ліжка (тривалість кількості прогнозованих діб воєнного конфлікту, що поділяється на середню тривалість лікування поранених, уражених, травмованих та хворих військовослужбовців (беруться показники від 30 до 60 діб).

Слід також узяти до уваги, що за сприятливої бойової та медико-тактичної обстановки на третьому рівні медичного забезпечення може залишатися до 45–50% від загальної кількості санітарних втрат [14].

Нормативи забезпечення медичних підрозділів військових частин (з'єднань) і військово-медичних закладів медичною технікою та майном, спеціальною медичною технікою під час їх застосування в особливий період установлені наказами Генерального штабу ЗСУ та Військово-медичного департаменту МОУ щодо організації медичного постачання в ЗСУ [24–28].

Водночас необхідно зазначити, що переліки медичного майна та спеціальної медичної техніки для військових частин (з'єднань) і військово-медичних закладів, установлені переліченими керівними документами, визначають норми та переліки медичного майна і спеціальної медичної техніки на період формування (утримання) військових частин (з'єднань) та військово-медичних закладів.

В умовах тривалих бойових дій військові частини (з'єднання) після виконання бойових завдань і понесення бойових втрат відводяться в райони відновлення боєздатності. У цей період проводиться поповнення запасів індивідуальних засобів медичного захисту, медичного майна (комплектів) спеціального призначення, поповнення втрат і відновлення спроможностей функціональних медичних комплектів.

Військово-медичні заклади потребують постійного поповнення запасів медичного майна, лікарських засобів, крові та її препаратів для забезпечення спроможності надання встановлених видів та обсягів медичної допомоги. Усі ці заходи проводяться за рахунок запасів медичного майна, які зберігаються на медичних складах, а також за рахунок лікарських засобів і витратного медичного майна військово-медичних клінічних центрів регіонів, у зоні відповідальності яких проходить відновлення боєздатності військових частин (з'єднань).

Під час визначення потреби в медичному майні необхідно враховувати, що:

- забезпеченість військових частин (з'єднань) засобами індивідуального медичного захисту має становити з розрахунку на 110% особового складу військової частини (з'єднання) [24];

- забезпеченість військових частин (з'єднань) та військово-медичних закладів комплектно-табельним оснащенням, медичним майном та спеціальною медичною технікою має відповідати встановленим керівними документами нормам [24–28];

- запаси індивідуальних засобів медичного захисту та медичного майна у військових частинах (з'єднаннях) і військово-медичних закладах мають забезпечувати покриття потреб непередбачуваних втрат медичного майна (близько 15% від потреби) та запасу медичного майна спеціального призначення (близько 20% від потреби) [14, 24].

Одним із завдань, визначених Стратегічним оборонним бюлетенем України, є створення необхідних запасів матеріально-технічних засобів для забезпечення обороноздатності держави [29], зокрема військового майна непорушних запасів, яке призначене для використання в особливий період і перебуває в мирний час на довгостроковому зберіганні у військових частинах, що регламентовано постановою Кабінету Міністрів України «Про затвердження Положення про порядок обліку, зберігання, списання та використання військового майна у Збройних Силах» [30].

Запаси медичного майна у ЗСУ поділяються на військові, оперативні та запаси центру [31].

Військові запаси призначені для формування та розгортання військових частин (з'єднань) та установ, переходу на штати воєнного часу і приведення їх у бойову готовність і перебувають безпосередньо у військових частинах (з'єднаннях) та установах. Вони розраховані здебільшого на одну військову операцію (3–5 діб). Поповнення військових запасів здійснюється за рахунок оперативних запасів, призначених для поповнення поточних витрат і бойових втрат військ (сил) при їх оперативному розгортанні та під час перших операцій (бойових дій).

Оперативні запаси формуються відповідно до норм запасів матеріально-технічних засобів для угруповань військ (сил) та зберігаються на складах і базах.

Запаси центру призначені для забезпечення нових формувань, компенсації безповоротних бойових втрат

матеріально-технічних засобів. Запаси центру створюються за планами Генерального штабу ЗСУ та є його резервом. За розрахунками, запаси центру мають забезпечити одно-тримісячну потребу військ (сил), які розпочали бойові дії.

Матеріальне забезпечення військ (сил) у перші місяці операцій (бойових дій) здійснюється з мобілізаційних запасів, які створюються в мирний час на період мобілізації оборонних галузей держави (економіки України). У подальшому забезпечення військ (сил) та військово-медичних закладів медичним майном і спеціальною медичною технікою має проводитися за рахунок їх поставок/закупівель від системи охорони здоров'я держави та інших міністерств і відомств (економіки України).

Важливим чинником забезпечення необхідних спроможностей Медичних сил є повне укомплектування військових частин (з'єднань) та санітарно-транспортних частин і підрозділів броньованими засобами для вивезення поранених, уражених і травмованих з поля бою, а також санітарно-транспортними засобами для медичної та аеромедичної евакуації. Водночас в умовах активних бойових дій та посиленої експлуатації санітарні автомобілі нерідко виходять з ладу внаслідок різних поломок, а іноді й знищуються противником, що потребує постійного їх ремонту (відновлення) та поповнення. Тому налагодження їх масового виробництва на вітчизняних промислових потужностях на умовах державного замовлення є вкрай важливим завданням. На жаль, на цей час таке виробництво, яке мало б забезпечувати потреби ЗСУ та інших складових сил оборони, в Україні відсутнє, а Медичні сили забезпечуються санітарно-транспортними засобами, спеціальною медичною технікою та польовими мобільними військово-медичними закладами за рахунок міжнародної технічної допомоги та волонтерів.

Підсумовуючи аналіз можливостей щодо ресурсного забезпечення потреб медичного забезпечення сил оборони необхідно зазначити, що крім власних ресурсів Медичних сил постановою Кабінету Міністрів України «Про затвердження мобілізаційних завдань (замовлень) на особливий період» [15] в інтересах медичного забезпечення сил оборони передбачене надання послуг від Укрзалізниці та Мінінфраструктури у проведенні медичної евакуації поранених, уражених, травмованих і хворих військовослужбовців, забезпечення Медичних сил і медичних служб інших складових сил оборони медичним майном, лікарськими засобами, кров'ю та її препаратами тощо. Крім того, порядок надання цих послуг на засадах єдиного медичного простору та їхні кількісні показники (обсяги) були регламентовані й деталізовані в постанові Кабінету Міністрів України «Про затвердження Воєнно-медичної доктрини України» [16], розпорядженні Кабінету Міністрів України «Деякі питання медичного забезпечення військовослужбовців, осіб рядового і начальницького складу та поліцейських, які беруть участь в антитерористичній операції та здійсненні заходів із

забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації у Донецькій та Луганській областях» [17] та спільному наказі МОУ та Міністерства охорони здоров'я України «Про визначення механізму надання вторинної (спеціалізованої) і третинної (високоспеціалізованої) медичної допомоги військовослужбовцям, які беруть участь в антитерористичній операції та здійсненні заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації та/або в умовах запровадження воєнного чи надзвичайного стану» [18].

Цей наказ визначає перелік закладів охорони здоров'я (253 заклади охорони здоров'я комунальної власності у 22 областях України), в яких майже 20 тис. профільних ліжок виділяються для надання медичної допомоги та лікування поранених, уражених, травмованих і хворих військовослужбовців, крім того, ще 1 тис. ліжок виділяється для зазначених цілей у 27 клінічних установах Національної академії медичних наук (НАМН) України.

Аналіз досвіду медичного забезпечення військ (сил) в умовах відбиття повномасштабної збройної агресії РФ проти України дає підстави стверджувати, що крім забезпечення потреб сил оборони в необхідній кількості медичних ресурсів визначальне значення мають їхні якісні характеристики і стан, які безпосередньо впливають на ефективність медичного забезпечення військ (сил), якість надання медичної допомоги на різних рівнях медичного забезпечення, збереження життя і здоров'я військовослужбовців та найскоріше повернення їх до військових частин після поранень, уражень і травм. Саме такі вимоги до медичного забезпечення сил оборони, серед інших, навів у своєму вечірньому зверненні до громадян України 19 листопада 2023 р. Президент України Володимир Зеленський [32].

Якість ресурсів для медичного забезпечення сил оборони має бути забезпечена та дотримана через:

- якісні й сертифіковані індивідуальні засоби медичного захисту (індивідуальні засоби надання першої медичної (домедичної) допомоги);
- якісне, сертифіковане, надійне та придатне до використання в польових умовах комплектно-табельне оснащення медичних підрозділів військових частин (з'єднань) та мобільних військово-медичних підрозділів і закладів;
- сучасні евакуаційно-транспортні засоби;
- якісну підготовку необхідної кількості стрільців-санітарів, бойових та старших бойових медиків у навчальних центрах (школах) ЗСУ відповідно до затверджених навчальних програм з тактичної медицини (TCCC – Tactical Combat Casualty Care);
- своєчасну та якісну медичну допомогу пораненим, ураженим, травмованим і хворим військовослужбовцям відповідно до стандартів медичної допомоги (медичних стандартів), ефективність яких відповідає міжнародним практикам.

Крім того, Міністр оборони України Рустем Умеров поставив перед Медичними силами ЗСУ завдання: «Життя і здоров'я наших поранених воїнів – це ваша особиста відповідальність. Ми маємо поєднати найновіші підходи НАТО з усім масивом досвіду бойових медиків з українського фронту... Вимагаю позбавитися застарілих практик, радянських підходів та всього, що не відповідає принципам НАТО. Вимагаю позбутися тонн паперу та нарешті зробити ефективну цифрову систему. Вимагаю зробити нормальний зворотний зв'язок з медиками на передку, щоб вони отримували все, що їм потрібно вчасно. Очікую чітких кроків для подолання означених проблем...» [33].

Досвід довготривалої повномасштабної війни РФ проти України підтвердив попередні розрахунки та напруження щодо необхідності створення в Україні власних промислових потужностей для виробництва і забезпечення потреб ЗСУ та інших складових сил оборони в медичному майні, лікарських засобах, комплектно-табельному і санітарно-технічному оснащенні та спеціальній медичній техніці шляхом укладання договорів за державним оборонним замовленням.

Наведені в статті законодавчі та нормативно-правові акти, керівні й доктринальні документи визначають порядок розрахунку потреби та формування необхідних ресурсів для медичного забезпечення ЗСУ. Водночас, крім планування та створення необхідних запасів медичних ресурсів, обов'язковою умовою успішного медичного забезпечення ЗСУ під час відбиття повномасштабної збройної агресії проти України є необхідність ефективного управління та раціонального використання медичних ресурсів.

Висновки

1. Установлено, що показники санітарних втрат особового складу військ (сил), а також принципи своєчасності, послідовності й наступності під час надання медичної допомоги пораненим, ураженим, травмованим і хворим військовослужбовцям є основними та визначальними чинниками під час розрахунку обсягів необхідних ресурсів для належного медичного забезпечення ЗСУ під час їх застосування.

2. Доведено, що для повноцінного медичного забезпечення ЗСУ Медичні сили повинні мати необхідний обсяг власних ресурсів, а в умовах відбиття повномасштабної збройної агресії проти України, крім того, необхідно залучати ресурси і послуги від системи охорони здоров'я держави та інших міністерств і відомств (економіки України).

3. Стверджується, що якість медичних ресурсів для медичного забезпечення сил оборони в умовах сучасних збройних конфліктів, зокрема й під час відбиття повномасштабної збройної агресії РФ проти України, має визначальне значення і безпосередньо впливає на ефективність медичного забезпечення військ (сил), якість надання медичної допомоги, збереження життя і здоров'я

військовослужбовців та найскоріше повернення їх до військових частин після поранень, уражень і травм.

4. Оборонне планування як основа розвитку та досягнення необхідних спроможностей сил оборони і забезпечення обороноздатності держави має бути основою для бюджетного фінансування сектору оборони відповідно до визначених ним переліку та обсягів необхідних ресурсів і послуг.

Перелік літератури

1. Про національну безпеку України [Електронний ресурс]: Закон України № 2469-VIII від 21 червня 2018 р. // Верховна Рада України. Законодавство України. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>.

2. Рекомендації з оборонного планування на основі спроможностей в Міністерстві оборони України та Збройних Силах України [Електронний ресурс]: затверджені Міністром оборони України 12 червня 2017 р. // Міністерство оборони України. – Режим доступу: https://www.mil.gov.ua/content/other/Recommendationson_CBP_120617.pdf.

3. Порядок організації та здійснення оборонного планування в Міністерстві оборони України, Збройних Силах України та інших складових сил оборони [Електронний ресурс]: наказ Міністерства оборони України № 484 від 22 грудня 2020 р. // Верховна Рада України. Законодавство України. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/z0196-21#Text>.

4. Доктрина «Управління оборонними ресурсами»: ВКП 8-00(03).01: затверджена Головнокомандувачем Збройних Сил України 13 листопада 2020 р. / Центральне управління оборонних ресурсів ГШ ЗС України, Центральний науково-дослідний інститут ЗС України. – [К.]: [б. в.], 2020. – 28 с.

5. Положення про Командування Медичних сил Збройних Сил України: наказ Головнокомандувача Збройних Сил України від 21 вересня 2020 р.

6. Стратегія розвитку Медичних сил Збройних Сил України до 2035 року: наказ Генерального штабу Збройних Сил України № 100 від 12 березня 2020 р.

7. Концепція програми розвитку системи медичного забезпечення Збройних Сил України на період до 2020 року [Електронний ресурс]: наказ Міністерства оборони України № 389 від 26 липня 2017 р. // Міністерство оборони України. – Режим доступу: https://www.mil.gov.ua/content/mou_orders/389_nm_2017.pdf.

8. Рекомендації з порядку організації проведення оцінювання спроможностей у Збройних Силах України: затверджені Міністром оборони України 7 грудня 2017 р.

9. Жаховський В. О. Планування на основі спроможностей: нова парадигма розвитку Медичних сил Збройних Сил України / В. О. Жаховський, В. Г. Лівінський // Український журнал військової медицини. – 2020. – Том 1, № 4. – С. 5–13.

10. Стратегія національної безпеки України [Електронний ресурс]: затверджена Указом Президента України № 392/2020 від 14 вересня 2020 р. // Верховна Рада України. Законодавство України. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/392/2020#Text>.

11. Стратегія воєнної безпеки України [Електронний ресурс]: затверджена Указом Президента України № 121/2021 від 25 березня 2021 р. // Верховна Рада України. Законодавство України. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/121/2021#Text>.

12. Методика розрахунку втрат особового складу військ (сил) на воєнний час : затверджена начальником Генерального штабу Збройних Сил України 6 червня 2011 р.

13. Методика розрахунку втрат особового складу на воєнний час : затверджена наказом Генерального штабу Збройних Сил України від 16 жовтня 2020 р.

14. Довідник оперативно-тактичних розрахунків з медичного забезпечення Збройних Сил України : ВП 3-35(42).01 : затверджений командувачем Медичних сил ЗС України 14 вересня 2020 р. / Командування Медичних сил ЗС України, Українська військово-медична академія. – [К.] : [б. в.], 2020. – 54 с.

15. Про затвердження мобілізаційних завдань (замовлень) на особливий період : постанова Кабінету Міністрів України від 5 грудня 2018 р.

16. Про затвердження Воєнно-медичної доктрини України [Електронний ресурс] : постанова Кабінету Міністрів України № 910 від 31 жовтня 2018 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/910-2018-p#Text>.

17. Деякі питання медичного забезпечення військовослужбовців, осіб рядового і начальницького складу та поліцейських, які беруть участь в антитерористичній операції та здійсненні заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації у Донецькій та Луганській областях [Електронний ресурс] : розпорядження Кабінету Міністрів України № 352-р від 24 травня 2017 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/352-2017-p#Text>.

18. Про визначення механізму надання вторинної (спеціалізованої) і третинної (високоспеціалізованої) медичної допомоги військовослужбовцям, які беруть участь в антитерористичній операції та здійсненні заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації та/або в умовах запровадження воєнного чи надзвичайного стану [Електронний ресурс] : наказ Міністерства оборони України та Міністерства охорони здоров'я України № 49/180 від 7 лютого 2018 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/z0252-18#Text>.

19. Про Збройні Сили України [Електронний ресурс] : Закон України № 1934-ХІІ від 6 грудня 1991 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/1934-12#Text>.

20. «Право на освіту не має бути причиною для уникнення призову», – Михайло Винницький про реформу вищої освіти в Україні [Електронний ресурс] // Радіо Культура. – Режим доступу : <http://nrcu.gov.ua/news.html?newsID=102783>.

21. Положення про проходження громадянами України військової служби у Збройних Силах України [Електронний ресурс] : затверджене Указом Президента України № 1153/2008 від 10 грудня 2008 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/1153/2008#n17>.

22. Про військовий обов'язок і військову службу [Електронний ресурс] : Закон України № 2232-ХІІ від 25 березня 1992 р. //

Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/2232-12#Text>.

23. Настанова з медичного забезпечення Збройних Сил України на особливий період, затверджена наказом Генерального штабу Збройних Сил України № 60 від 11 лютого 2019 р.

24. Про затвердження Переліку медичного майна та техніки, які постачаються Збройним Силам України на особливий період : наказ Генерального штабу Збройних Сил України від 30 червня 2015 р. (зі змінами).

25. Про затвердження Збірника описів комплектів медичного майна для військових частин та закладів Збройних Сил України і Порядку переформування комплектів медичного майна : наказ Генерального штабу Збройних Сил України від 30 червня 2015 р.

26. Про внесення змін до наказу Генерального штабу Збройних Сил України : наказ Генерального штабу Збройних Сил України № 7 від 7 січня 2017 р.

27. Про затвердження Тимчасового переліку та обсягів медичного майна для лікування поранених та хворих на особливий період : наказ Генерального штабу Збройних Сил України від 3 липня 2015 р.

28. Про затвердження норм постачання медичним майном військових мобільних госпіталів : наказ директора Військово-медичного департаменту Міністерства оборони України № 18 від 3 листопада 2017 р.

29. Стратегічний оборонний бюлетень України [Електронний ресурс] : затверджений Указом Президента України № 473/2021 від 17 вересня 2021 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/473/2021#n17>.

30. Положення про порядок обліку, зберігання, списання та використання військового майна у Збройних Силах [Електронний ресурс] : постанова Кабінету Міністрів України № 1225 від 4 серпня 2000 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/1225-2000-p#n11>.

31. Організація забезпечення медичним майном військових частин і медичних установ в умовах надзвичайного стану : навч. посібник для студентів вищ. мед. і фармац. навч. закладів III–IV рівнів акредитації / П. С. Сирота, В. В. Трохимчук, В. І. Гридасов та ін. – Х. : Вид-во НФаУ : Золоті сторінки, 2002. – 320 с.

32. Потрібен принципово новий рівень медичного забезпечення воїнів – звернення Президента України [Електронний ресурс] : 19 листопада 2023 р. // Президент України. Офіційне інтернет-представництво. – Режим доступу : <https://www.president.gov.ua/news/potriben-principovo-novij-riven-medichnogo-zabezpechennya-vo-87137>.

33. Рустем Умеров представив військовим медикам новопризначеного командувача Медичних сил Збройних Сил України [Електронний ресурс] // АрміяInform. – Режим доступу : <https://armyinform.com.ua/2023/12/01/rustem-umyerov-predstavyyv-vijskovym-medyam-novopryznachenogo-komandu-vacha-medychnyh-syl-zbrojnyh-syl-ukrayiny>.

DOI 10.33099/2618-1614-2023-23-4-14-22

УДК 355.232.6:378.1

А. В. Слюсаренко,*доктор історичних наук, професор,
заступник начальника університету з навчальної роботи,
Національний університет оборони України, полковник,***В. М. Телелим,***доктор військових наук, професор,
професор кафедри стратегії національної безпеки та оборони,
Національний університет оборони України,***А. М. Зельницький,***кандидат педагогічних наук, професор, провідний науковий
співробітник центру воєнно-стратегічних досліджень,
Національний університет оборони України,***О. А. Заболотний,***кандидат військових наук, доцент, провідний науковий
співробітник центру воєнно-стратегічних досліджень,
Національний університет оборони України*

Забезпечення якості професійної військової освіти: визначення понять і моніторинг поточного стану

У статті проаналізовано й уточнено окремі компоненти поняттєво-категоріального апарату у сфері забезпечення якості професійної військової освіти в Україні, запропоновано структуру системи забезпечення якості професійної військової освіти, показники оцінювання її стану, а також розглянуто підходи до здійснення моніторингу якості професійної військової освіти з урахуванням вітчизняного досвіду й досвіду країн – членів НАТО.

Ключові слова: вища освіта, професійна військова освіта, забезпечення якості, моніторинг якості, гарантування якості.

© А. В. Слюсаренко, В. М. Телелим, А. М. Зельницький,
О. А. Заболотний, 2023

Постановка проблеми. Повномасштабне збройне вторгнення РФ на територію України і ведення силами безпеки та оборони нашої держави довготривалих виснажливих бойових дій із захисту територіальної цілісності та незалежності батьківщини стали одним з головних чинників, що визначили необхідність прискорення реалізації стратегічного курсу України на набуття повноправного членства в Європейському Союзі та Організації Північноатлантичного договору, суттєвої активізації в максимально стислі строки реформ, визначених в [1], що значною мірою сприятиме відновленню територіальної цілісності України, виведенню російських військ та припиненню бойових дій. Нині виникла нагальна потреба в поступовому переході до засад професійної армії, невідкладному її забезпеченні боєздатними, мобільними, висококваліфікованими, вмотивованими офіцерськими кадрами з глибокими професійними знаннями, спроможними виконувати завдання із захисту країни, діяти спільно з підрозділами країн Альянсу, приймати відповідальні рішення в ситуаціях вибору, а також вирізнятися мобільністю, динамізмом, конструктивізмом, критичним мисленням, здатністю реалізовувати свої професійні та творчі здібності в екстремальних умовах службової діяльності, що передбачає нові підходи до формування структури і змісту системи військової освіти [2]. Отже, значно актуалізувалася проблема всебічного забезпечення і гарантування якості військової освіти та її найважливішої складової – професійної військової освіти в умовах введення в Україні воєнного стану.

Метою статті є систематизоване викладення поглядів авторів на розроблення й впровадження в освітню діяльність вищих військових навчальних закладів (ВВНЗ) інноваційних підходів до управління процесом забезпечення і гарантування якості професійної військової освіти (ПВО).

Огляд новітніх досліджень і публікацій. Актуальні проблеми забезпечення якості освіти розглядаються у відповідних нормативно-правових актах [1–4], наукових працях вітчизняних та зарубіжних учених-педагогів та психологів А. Василюка, В. Кременя, В. Лугового, Т. Лукиної, Л. Одерія, О. Овчарука, О. Отича, О. Ніколаєнка, Т. Рогової, D. Green, L. Harvey, J. Parri та ін. Вагомий внесок у розв'язання проблеми забезпечення й гарантування якості вищої військової освіти, впровадження в освітній процес інноваційних педагогічних технологій і методик, сучасних методів моніторингу, цифровізації освіти тощо здійснили українські військові вчені А. Вітченко, А. Кучерявий, А. Лобанов, О. Майстренко, В. Медведєв, С. Микусь, В. Мірненко, М. Нецадим, Л. Олійник, В. Осьодло, Б. Семон, Ю. Пунда, В. Рахманов, Ю. Репіло, В. Рижиков, В. Телелим, П. Щипанський, В. Ягупов та ін.

Аналіз досліджень і публікацій згаданих авторів значною мірою сприяв розробленню інноваційних підходів до розв'язання проблеми управління процесом забезпечення якості професійної військової освіти із застосуванням

методів експертного опитування та кількісного оцінювання його результатів.

Виклад основного матеріалу. Будь-яке теоретичне дослідження актуальних проблем у певній галузі знань передусім потребує опису, аналізу й уточнення відповідних понять. Це повною мірою стосується й військової освіти, яка нині перебуває під постійним впливом змінюваних у часі й просторі чинників зовнішнього і внутрішнього середовищ, а отже, потребує структурного і змістового вдосконалення основних її складових, у тому числі приведення поняттєво-категоріального апарату у відповідність до сучасних запитів військової науки та освіти. Подібне вдосконалення має відбуватися на основі системного аналізу і здійснюватися за певними алгоритмом, зокрема:

- введення в науковий обіг нормативно не визначених понять;
- уточнення змісту нормативно визначених понять;
- адаптація змісту загальноосвітніх понять до специфіки військової освіти;
- забезпечення взаємосумісності (гармонізації) понять, застосовуваних у вітчизняній нормативно-правовій базі зі стандартами країн – членів НАТО.

У даній статті увага акцентується на аналізі й уточненні таких базових категорій:

- професійна військова освіта;
 - якість професійної військової освіти;
 - забезпечення якості професійної військової освіти;
 - моніторинг якості професійної військової освіти,
- а також дотичних до них термінів, що чинять безпосередній вплив на змістове наповнення базових категорій.

Професійна військова освіта

Поняття «професійна військова освіта» в «Концепції трансформації системи військової освіти» [2] і в Законі України «Про освіту» [3] представлене однаково – як спеціалізована освіта військового спрямування, яка здобувається за освітніми програмами на відповідних рівнях військової освіти з метою вдосконалення професійного рівня військового фахівця та набуття фахових компетентностей, що забезпечують виконання службових (бойових) функцій. Наведене поняття потребує, на нашу думку, певних уточнень, які дадуть змогу чіткіше визначити сутність професійної військової освіти, основні її складові, зв'язки між ними та пріоритети подальшого розвитку професійної військової освіти. Для цього необхідно:

по-перше, конкретизувати суб'єктів ПВО – це військові фахівці сил безпеки та оборони України;

по-друге, розглядати ПВО в контексті безперервності освіти й тісного її взаємозв'язку з кар'єрним зростанням військових фахівців;

по-третє, акцентувати увагу цілеспрямованості ПВО на гарантоване досягнення запланованих результатів навчання відповідно до стандартів освіти;

по-четверте, наголосити на пріоритетності набуття сумісності ПВО України з відповідною підготовкою

військових фахівців збройних сил держав – членів НАТО;

і по-п'яте, відійти від подвійного використання терміна «рівень», застосовуваного і до процесів, і до об'єктів освітньої діяльності.

Ураховуючи зазначене, автори пропонують викласти поняття «*професійна військова освіта*» в такій редакції: це неформальна, спеціалізована освіта військового спрямування з підготовки військових фахівців сил безпеки та оборони України, яка здобувається за освітніми програмами на відповідних рівнях освіти, базується на безперервності освітнього процесу й тісному взаємозв'язку з кар'єрним зростанням військових фахівців і спрямована на гарантоване досягнення ними запланованих результатів навчання згідно з вимогами вітчизняних стандартів, гармонізованих з відповідними стандартами країн – членів НАТО, що має забезпечити ефективне виконання військовими фахівцями службових (бойових) функцій на посадах призначення в умовах мирного часу та в особливий період.

Якість професійної військової освіти

Поняття «*якість професійної військової освіти*» в нормативній базі не визначене.

У Законі України «Про освіту» якість освіти – це відповідність результатів навчання вимогам, установленим законодавством, відповідним стандартом освіти та/або договором про надання освітніх послуг [3]. Узагалі існують різні підходи до тлумачення поняття «якість освіти» [5–8], які можна інтегрувати за такими узагальненими показниками: результативність, процесуальність, комплексність, ефективність. При цьому варто зазначити, що якість освіти може відбивати як сучасні потреби, так і бути націленою на майбутнє з урахуванням тенденцій її розвитку.

У новій редакції Закону України «Про вищу освіту» якість вищої освіти – це «відповідність умов провадження освітньої діяльності та результатів навчання вимогам законодавства та стандартам вищої освіти, професійним та/або міжнародним стандартам (за наявності), а також потребам заінтересованих сторін і суспільства, що забезпечується шляхом здійснення процедур внутрішнього та зовнішнього забезпечення якості» [4]. При цьому «освітня діяльність – діяльність закладів вищої освіти, спрямована на організацію, забезпечення та реалізацію освітнього процесу», де основними видами забезпечення цієї діяльності є кадрове, навчально-методичне, матеріально-технічне, інформаційне тощо.

Базуючись на результатах аналізу нормативно-правових актів, енциклопедичних словникових та інших літературних джерел стосовно категорії «якість», пропонується таке визначення поняття якості ПВО.

«*Якість професійної військової освіти*» – це ступінь відповідності умов провадження освітньої діяльності та результатів підготовки фахівців сил безпеки та оборони України вимогам чинного законодавства та професійним

вітчизняним і міжнародним стандартам (стандартам країн – членів НАТО), а також потребам стейкхолдерів і суспільства, що забезпечується шляхом підготовки фахівців у системі професійної військової освіти зі здобуттям ними відповідних рівнів освіти (тактичного, оперативного, стратегічного).

Забезпечення якості професійної військової освіти

Поняття «забезпечення якості освіти» як базове в Законах України «Про освіту» та «Про вищу освіту» взагалі відсутнє, хоча частково представлене певними структурними складниками. При цьому жодним чином не згадується про результати цього процесу як основну мету забезпечення якості освіти, хоча на теперішній час країни Болонського процесу практично повністю перейшли до моделі забезпечення якості на основі результатів, де основна увага приділяється визначенню чітко вимірюваних критеріїв та індикаторів якості [1], що знайшло певне відображення у матеріалах даної статті.

Отже, поняття «забезпечення якості професійної військової освіти», на нашу думку, є процесом створення центральними органами виконавчої влади, органами управління військовою освітою, закладами (структурами) військової світи та іншими зацікавленими сторонами надійних умов здійснення ефективного освітнього процесу та освітньої діяльності й постійного їх підтримання в належному стані з метою гарантованого досягнення фахівцями сил безпеки та оборони України запланованих результатів навчання, сформованості визначених компетентностей, інших професійно важливих якостей і ціннісних орієнтацій. У наведеному визначенні є дві ключові компоненти – створення та підтримання надійних умов освітнього процесу і результати навчання, що віддзеркалюють сутність даного поняття.

Дотичними до даного поняття є «компетентність здобувача вищої військової освіти» і «гарантування якості професійної військової освіти», які в нижче представлених авторами визначеннях можуть бути запропоновані до введення в науковий обіг сфери військової освіти.

Компетентність здобувача вищої військової освіти – показник якості його підготовки як систематично підтверджувана ним здатність до постійного самовдосконалення й самоосвіти та готовність до виконання функціональних обов'язків на посаді призначення у військах (силах) в умовах мирного часу та в особливий період на основі творчого застосування здобутих знань, сформованих навичок та вмінь, інших професійно важливих якостей і ціннісних орієнтацій відповідно до вимог вітчизняних і міжнародних стандартів освіти (стандартів НАТО). У наведеному визначенні поняття порівняно з раніше застосовуваними [4; 6; 9] варто звернути увагу на словосполучення «систематично підтверджувана ним (здобувачем освіти) здатність». Тобто принцип «здав – забув» уже не спрацьовує, що вимагає постійного здійснення процедур діагностування педагогами й самодіагностування здобувачами освіти рівнів сформованості в них

професійно важливих якостей і ціннісних орієнтацій у процесі проведення відповідних моніторингових досліджень щодо забезпечення й гарантування якості освіти.

Гарантування якості професійної військової освіти – це порука й відповідальність органів управління військовою освітою та закладів (структур) військової світи за виконання ними державного замовлення на підготовку особового складу сил безпеки та оборони України з досягненням запланованих результатів навчання (сформованості визначених компетентностей), здобуттям відповідних рівнів військової освіти (тактичного, оперативного, стратегічного) у визначені терміни та формуванням у здобувачів освіти необхідних спроможностей щодо ефективного виконання ними службово-бойових функцій на посадах призначення у військах (силах) в умовах мирного часу і воєнного стану.

Таким чином, одержані результати аналізу зазначених понять категоріального апарату у сфері вищої освіти, їх адаптація до особливостей ПВО склали підґрунтя для вироблення пропозицій з розв'язання визначеної в статті проблеми забезпечення якості професійної військової освіти з урахуванням еволюції поглядів на її функціонування в Україні й у НАТО.

Відповідно до статті 16 розділу V Закону України «Про вищу освіту» [4] система забезпечення якості вищої освіти в Україні складається із:

- 1) системи забезпечення закладами вищої освіти якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості);
- 2) системи зовнішнього забезпечення якості освітньої діяльності закладів вищої освіти та якості вищої освіти;
- 3) системи забезпечення якості діяльності Національного агентства із забезпечення якості вищої освіти і незалежних установ оцінювання та забезпечення якості вищої освіти.

Система забезпечення закладами вищої освіти якості освітньої діяльності та якості вищої освіти (система внутрішнього забезпечення якості) передбачає здійснення таких процедур і заходів:

- 1) визначення принципів і процедур забезпечення якості вищої освіти;
- 2) здійснення моніторингу та періодичного перегляду освітніх програм;
- 3) щорічне оцінювання здобувачів вищої освіти, науково-педагогічних і педагогічних працівників закладу вищої освіти та регулярне оприлюднення результатів таких оцінювань на офіційному веб-сайті закладу вищої освіти, на інформаційних стендах та в будь-який інший спосіб;
- 4) забезпечення підвищення кваліфікації педагогічних, наукових і науково-педагогічних працівників;
- 5) забезпечення наявності необхідних ресурсів для організації освітнього процесу, в тому числі самостійної роботи студентів, за кожною освітньою програмою;
- 6) забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;

7) забезпечення публічності інформації про освітні програми, ступені вищої освіти та кваліфікації;

8) забезпечення дотримання академічної доброчесності працівниками закладів вищої освіти та здобувачами вищої освіти, в тому числі створення й забезпечення функціонування ефективної системи запобігання та виявлення академічного плагіату;

9) інших процедур і заходів.

Система зовнішнього забезпечення якості освітньої діяльності закладів вищої освіти та якості вищої освіти передбачає здійснення таких процедур і заходів:

1) забезпечення ефективності процесів і процедур внутрішнього забезпечення якості освітньої діяльності закладів вищої освіти та якості вищої освіти;

2) забезпечення наявності системи проведення процедур зовнішнього забезпечення якості;

3) забезпечення наявності оприлюднених критеріїв прийняття рішень відповідно до стандартів і рекомендацій забезпечення якості в Європейському просторі вищої освіти;

4) налагодження доступного і зрозумілого звітування;

5) проведення періодичних перевірок діяльності систем забезпечення якості та механізмів роботи з отриманими рекомендаціями;

6) інших процедур і заходів.

Розгляньмо зміст представлених структурних складових внутрішнього забезпечення якості ПВО в контексті подальшого здійснення процедур вимірювання та оцінювання її поточного стану (рис. 1):

1. Кадрове забезпечення:

1) якість науково-педагогічних працівників (НПП) і стан укомплектованості ними штатних посад;

2) академічна мобільність НПП;

3) забезпечення якості підготовки НПП на курсах підвищення кваліфікації;

4) якість застосовуваної рейтингової системи оцінювання професійної діяльності учасників освітнього процесу;

5) організація набору кандидатів на навчання в заклади військової освіти за спеціальностями і спеціалізаціями відповідно до результатів професійного відбору;

6) академічна мобільність здобувачів освіти;

7) забезпечення надлишкового набору кандидатів на вступ до ВВНЗ із урахуванням імовірності їх відрахування за неуспішністю навчання та іншими чинниками.

2. Правове забезпечення:

1) відповідність нормативно-правових актів України потребам сил безпеки та оборони;

2) відповідність відомих керівних документів сучасним потребам закладів військової освіти;

3) оперативність внесення обґрунтованих пропозицій учасниками освітнього процесу у внутрішні нормативні акти ВВНЗ.

3. Матеріально-технічне забезпечення:

1) відповідність стану матеріально-технічної бази за місцем дислокації закладів військової освіти нормативним вимогам;

2) відповідність стану польової матеріальної бази закладів військової освіти нормативним вимогам.

4. Навчально-методичне та наукове забезпечення:

1) відповідність змісту програм ПВО вимогам стандартів професійної військової освіти, вимогам замовників на підготовку військових фахівців, потребам військ, зацікавлених сторін і стандартам НАТО;

2) оперативність корегування змісту робочих програм навчальних дисциплін відповідно до потреб замовників з урахуванням пропозицій слухачів відповідних рівнів підготовки;

3) відповідність застосовуваних методик навчання і педагогічних технологій сучасним освітнім практикам;

4) забезпечення періодичності оцінювання та вимірювання результатів підготовки слухачів (визначення рівня сформованості передбачених компетентностей) після завершення освітньо-професійної програми або окремих освітніх компонентів;

5) ефективність застосовуваної бально-рейтингової системи оцінювання діяльності слухачів;

6) відповідність якості надання НПП консультативних послуг освітнім потребам слухачів;

7) організація вивчення іноземних (англійської) мов;

8) постійне впровадження в освітній процес сучасних досягнень у сфері науки (воєнної науки) і техніки.

Навчально-методичне забезпечення є найважливішою складовою структури забезпечення якості професійної військової освіти, головним компонентом якої є освітні програми ПВО з підготовки слухачів на тактичному, оперативному і стратегічному рівнях (курси L-1–L-5), що ретельно розглянуто в Концепції трансформації системи військової освіти [2].

Основною формою здобуття ПВО є очне навчання. Програми ПВО, що реалізуються за різними моделями, методиками і технологіями, мають гарантовано забезпечувати визначений рівень результатів навчання, які можна ідентифікувати, спланувати, оцінити і виміряти та які особа здатна продемонструвати після завершення освітньої програми або окремих освітніх компонентів.

Програми ПВО спрямовані здебільшого на формування практичних навичок, необхідних для виконання службових обов'язків на посадах у військах (силах) та навичок критичного мислення. При цьому методики й технології навчання мають співвідноситися з теоретичними і практичними знаннями, одержаними слухачами під час здобуття ступеня вищої освіти, орієнтуючи їх на аналіз і розв'язання проблем, пов'язаних передусім з їхньою здатністю і готовністю до застосування сформованих компетентностей на посадах призначення у військах (силах) в умовах особливого періоду [10–12].

5. Фінансово-економічне забезпечення:

1) відповідність фінансування освітньої діяльності потребам ВВНЗ;

2) безпосереднє залучення додаткових коштів у ВВНЗ, військові навчальні підрозділи закладів вищої

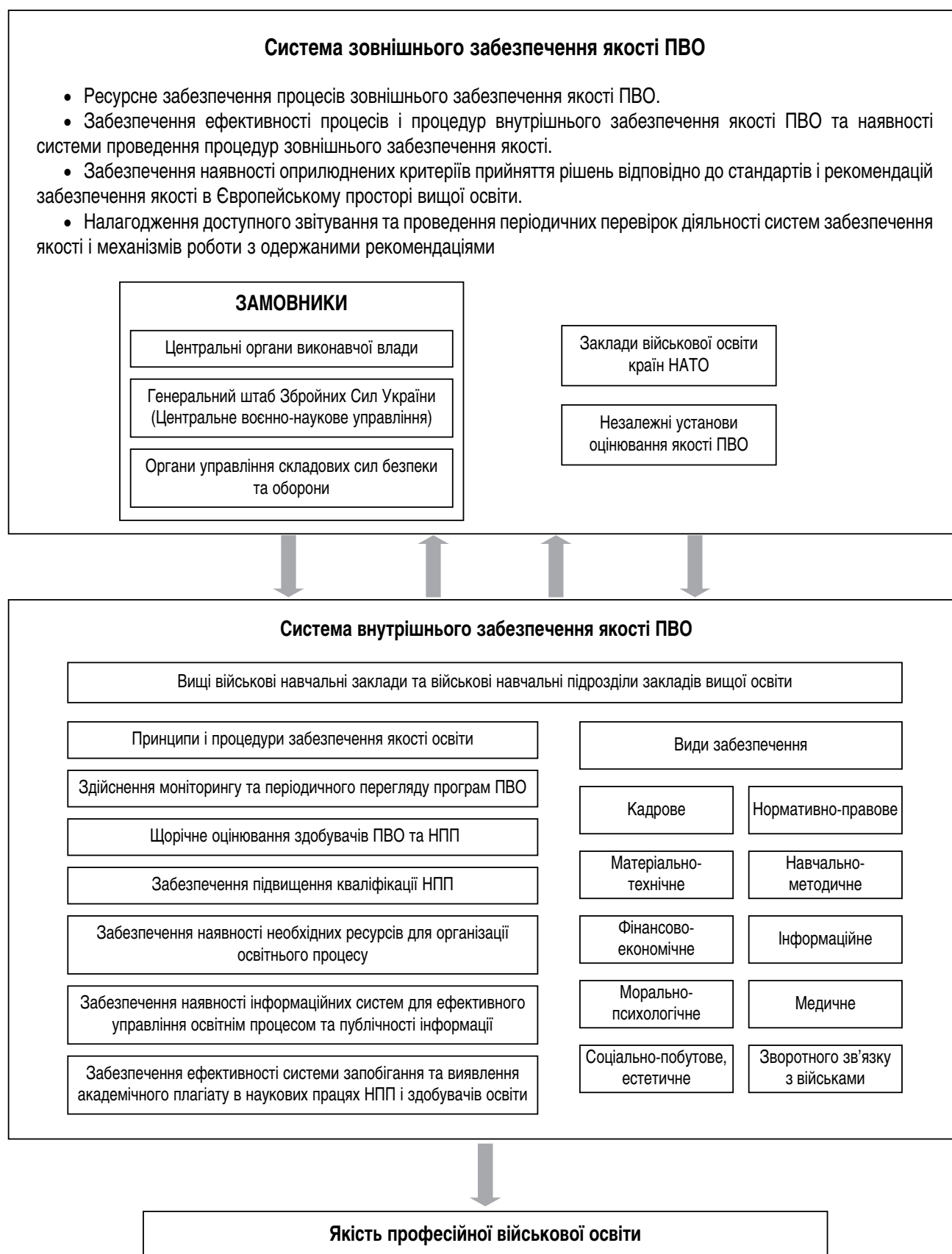


Рис. 1. Структура системи забезпечення якості професійної військової освіти

освіти (ВНП ЗВО) (внески вітчизняних і зарубіжних благодійних та спонсорських організацій);

3) матеріальне стимулювання учасників освітнього процесу за особливо вагомий внесок в освітню, наукову, інноваційну діяльність, сумлінне виконання функціональних обов'язків, термінових доручень (оперативних завдань), наказів, успішне керівництво підпорядкованими структурними підрозділами.

6. Інформаційне забезпечення:

1) моніторинг функціонування єдиної інформаційної системи у ВВНЗ, ВНП ЗВО як програмно-апаратного комплексу для ефективного управління освітньою діяльністю закладів військової освіти та здійснення відповідного корегування цієї системи;

2) оприлюднення інформації про програми ПВО, рівні освіти і кваліфікації та результати освіти, про проведення наукових конференцій тощо;

3) наявність у бібліотечному фонді вітчизняних та закордонних фахових періодичних видань за напрямками підготовки (в електронній і паперовій формах) та електронних каталогів відповідно до потреб учасників освітнього процесу;

4) оперативність надання бібліотечних послуг учасникам освітнього процесу.

7. Морально-психологічне забезпечення:

1) Сприятливість морально-психологічного клімату (МПК) у первинному навчальному колективі;

2) сприятливість МПК у закладі військової освіти та його структурних підрозділах.

8. Забезпечення усталеного зворотного зв'язку:

1) з військами (силами) – відгук з військ на випускника закладу військової освіти (після першого року служби на посаді призначення);

2) із замовниками на підготовку військових фахівців (постійно);

3) зі здобувачами військової освіти (постійно);

4) з НПП (постійно).

9. Соціально-побутове та естетичне забезпечення – створення належних умов:

1) проживання;

2) харчування;

3) санітарно-гігієнічних;

4) естетичних.

10. Медичне забезпечення:

1) своєчасність та якість надання медичних послуг;

2) підтримання здоров'я учасників освітнього процесу та вжиття заходів з його зміцнення.

Розроблена на засадах системного підходу структура системи забезпечення якості професійної військової освіти відповідає стандартам і рекомендаціям щодо забезпечення якості освіти в Україні та Європейському просторі вищої освіти і є підґрунтям для подальшого її впровадження в педагогічну практику закладів військової освіти, що має сприяти:

• ефективній централізованій підготовці особового складу сил безпеки та оборони України з урахуванням вимог стандартів НАТО;

• реалізації принципу «освіта впродовж військової кар'єри»;

• взаємовизнанню сертифікатів, отриманих у військових навчальних закладах України та в державах – членах НАТО [13].

Процес забезпечення якості ПВО має постійно моніторитися, що передбачає застосування певних процедур, які дають відповідь на два основні запитання: 1) наскільки одержані результати моніторингу відповідають бажаному стану системи (відхилень від нього)? і 2) як використовувати одержані результати для прийняття обґрунтованих управлінських рішень?

У межах розв'язання порушеної в статті проблеми забезпечення якості ПВО запропоновано використання методів експертних оцінок, заснованих на результатах аналітичної діяльності експертної групи. До складу експертної групи з оцінювання стану забезпечення якості ПВО мають обов'язково входити представники замовників на підготовку військових фахівців, делеговані представники слухацьких і педагогічних колективів та інші учасники освітнього процесу (*реалізація принципу демократизації військової освіти*), представники незалежних структур оцінювання, зацікавлені в одержанні об'єктивних результатів.

Експертне оцінювання рівня забезпечення якості ПВО доцільно здійснювати за вже апробованим алгоритмом із застосуванням спеціально розроблених опитувальників [14, с. 81–85].

У наведеному опитувальнику (*табл. 1*) представлені види забезпечення якості ПВО та показники, за якими вони оцінюються.

Прояв кожного з наведених показників пропонується оцінювати експертам із застосуванням 10-бальної шкали шляхом внесення позначки «V» у певні стовпчики *таблиці 1*.

При цьому:

• бал 10 – прояв показника, що, на думку експерта, абсолютно відповідає встановленим вимогам до забезпечення якості ПВО (100%) – найвищий рівень;

• діапазон балів 8–9 – прояв показника, що цілком відповідає вимогам (80–90%) – високий рівень;

• діапазон балів 7–8 – прояв показника, що більшою мірою відповідає вимогам (70–80%) – рівень близький до високого;

• діапазон балів 6–7 – прояв показника, що скоріш відповідає, ніж не відповідає вимогам (60–70%) – середній рівень;

• діапазон балів 5–6 – прояв показника, що характеризує гранично припустимий рівень (50–60%);

• діапазон балів 1–4 – прояв показника, що більшою мірою не відповідає встановленим вимогам до забезпечення якості ПВО (10% – 40%) – неприпустимий рівень;

Таблиця 1

Опитувальник з оцінювання рівня забезпечення якості ПВО

Види забезпечення якості професійної військової освіти та показники оцінювання їхнього рівня	Значення показників за 10-бальною шкалою										
	0	1	2	3	4	5	6	7	8	9	10
1. Кадрове забезпечення											
1. Стан укомплектованості посад НПП (якість НПП, відповідність заповнення вимогам штату)											
2. Академічна мобільність НПП											
3. Забезпечення якості підготовки НПП на курсах підвищення кваліфікації											
4. Якість застосовуваної рейтингової системи оцінювання професійної діяльності НПП											
5. Академічна мобільність здобувачів освіти											
6. Якість професійного відбору кандидатів на навчання											
7. Забезпечення надлишкового набору кандидатів на вступ до ВВНЗ із урахуванням імовірності їх відрахування за неуспішністю навчання											
2. Правове забезпечення											
1. Відповідність нормативно-правових актів України потребам сил безпеки та оборони											
2. Відповідність відомчих документів потребам ВВНЗ											
3. Своєчасність внесення змін у нормативно-правові акти											
3. Матеріально-технічне забезпечення											
1. Стан матеріально-технічної бази за місцем дислокації											
2. Стан польової матеріально-технічної бази											
4. Навчально-методичне та наукове забезпечення											
1. Відповідність змісту освітніх програм вимогам замовників											
2. Відповідність змісту освітніх програм потребам здобувачів освіти											
3. Моніторинг якості підготовки слухачів											
4. Рівень організації мовної підготовки (англійська мова)											
5. Застосовуваних інноваційних педагогічних технологій											
6. Надання якісних консультативних послуг науково-педагогічними працівниками слухачам											
7. Упровадження сучасних досягнень науки в освітній процес											
5. Фінансово-економічне забезпечення											
1. Відповідність фінансування освітньої діяльності потребам ВВНЗ та ВВП ЗВО											
2. Залучення додаткових коштів вітчизняних і зарубіжних благодійних та спонсорських організацій											
3. Матеріальне стимулювання учасників освітнього процесу за особливо вагомий внесок в освітню та наукову діяльність											
6. Інформаційне забезпечення											
1. Моніторинг функціонування єдиної інформаційної системи управління освітньою діяльністю											
2. Наявність у бібліотечному фонді електронних і паперових вітчизняних та закордонних фахових періодичних видань											
3. Оперативність надання бібліотечних послуг											
4. Оприлюднення інформації на сайті ВВНЗ про рівні освіти і кваліфікації та про освітню, наукову й інші види діяльності											

Продовження таблиці 1

Види забезпечення якості професійної військової освіти та показники оцінювання їхнього рівня	Значення показників за 10-бальною шкалою										
	0	1	2	3	4	5	6	7	8	9	10
7. Морально-психологічне забезпечення											
1. Сприятливість морально-психологічного клімату в первинному навчальному колективі щодо здійснення освітньої діяльності											
2. Сприятливість морально-психологічного клімату у ВВНЗ											
8. Забезпечення зворотного зв'язку											
1. З військами (силами) – відгук з військ на випускника											
2. Із замовником на підготовку військових фахівців											
3. Зі слухачами											
4. З НПП											
9. Соціально-побутове забезпечення											
1. Умови проживання											
2. Умови харчування											
3. Санітарно-гігієнічні умови											
4. Естетичні умови											
10. Медичне забезпечення											
1. Оперативність надання необхідних медичних послуг											
2. Підтримання здоров'я учасників освітнього процесу та вжиття заходів з його зміцнення											
Узагальнений показник											

• 0 балів – експерт не може оцінити прояв показника.

Заповненню опитувальника передують колективне обговорення членами експертної групи (під керівництвом менеджера) структури системи забезпечення якості ПВО і внесення в неї певних пропозицій від експертів, особливо стосовно відповідності змісту кожного з показників видам забезпечення та оптимальності обсягів наповнення (первинне корегування).

За результатами заповнення опитувальників проводяться відповідні процедури оцінювання рівня забезпечення якості ПВО, що реалізуються з використанням теорії кваліметрії, алгоритм і практичне впровадження яких у педагогічну практику військової освіти представлені в зазначених літературних джерелах [9, с. 42; 14, с. 247].

Результати опитування в балах (табл. 1) для кожного виду забезпечення за кожним з показників K_i (де i – номери показників усередині виду забезпечення) співвідносяться з балом «10» – еталонним значенням прояву показника – та підраховуються за формулою переходу від абсолютних (бальних) до відносних показників:

$$K_{ij} = \frac{P_{ij}}{P_j^{\text{ет}}} \quad (1)$$

де K_{ij} – відносне значення прояву i -го показника за результатами опитування j -го експерта;

P_{ij} – абсолютне значення прояву i -го показника, вказане в опитувальнику j -м експертом, – від балу «1» до балу «10»;

$P_j^{\text{ет}}$ – еталонне значення прояву i -го показника – бал «10».

Далі підраховується $K_i^{\text{ср}}$ – середньоарифметичне відносне значення прояву i -го показника за результатами його оцінювання всіма експертами групи:

$$K_{i\text{ср}} = \frac{\sum_{j=1}^n K_{ij}}{n}, \quad (2)$$

де n – кількість експертів в експертній групі.

Такий підхід дає змогу визначити як інтегральні показники рівня забезпечення якості ПВО за його видами, так і узагальнений показник рівня забезпечення якості ПВО (K_{Σ}):

$$K_{\Sigma} = \frac{\sum_{i=1}^m K_{i\text{ср}}}{m}, \quad (3)$$

де m – загальна кількість оцінених показників.

Організоване подібним чином експертне оцінювання є підґрунтям для проведення комплексного аналізу результатів забезпечення якості професійної військової освіти з подальшим корегуванням освітньої діяльності та освітнього процесу закладів військової освіти і впровадженням

на їхній основі обґрунтованих управлінських рішень у педагогічну практику.

Висновки

У статті за результатами проведеного аналізу особливостей змісту та специфіки функціонування системи забезпечення якості професійної військової освіти представлені відповідні підходи до розв'язання нагальних проблем ПВО, зокрема:

1. Запропоновано до введення в науковий обіг такі базові поняття системи забезпечення якості професійної військової освіти: «професійна військова освіта»; «якість професійної військової освіти»; «забезпечення якості професійної військової освіти»; «компетентність здобувача військової освіти», «гарантування якості професійної військової освіти», які на сьогодні законодавчо не визначені або не адаптовані до особливостей функціонування системи професійної військової освіти.

2. Розроблено структуру системи забезпечення якості професійної військової освіти, яка охоплює десять основних видів забезпечення, зокрема: кадрове, нормативно-правове, матеріально-технічне, навчально-методичне та наукове, фінансово-економічне, інформаційне, морально-психологічне, зворотного зв'язку, соціально-побутове та естетичне, медичне, кожен з яких диференційований на відповідні показники, що склало підґрунтя для розгляду ПВО як цілісного системного утворення.

3. Викладено підходи до об'єктивізації процедур вимірювання та оцінювання поточного стану ПВО із застосуванням теорії кваліметрії, розроблено рекомендації щодо здійснення моніторингу ефективності функціонування системи забезпечення якості професійної військової освіти, що може слугувати основою для вдосконалення управлінської діяльності ВВНЗ та ВВП ЗВО, спрямованої на гарантоване досягнення найвищих результатів у підготовці військових фахівців сил безпеки та оборони України.

Подальші дослідження щодо комплексного розв'язання зазначеної проблеми доцільно спрямувати на впровадження в педагогічну практику ВВНЗ, ВВП ЗВО рекомендованих у статті підходів у процесі підготовки військових фахівців сил безпеки та оборони України, створивши для цього в кожному вищому військовому навчальному закладі окремий структурний підрозділ із забезпечення якості освіти та освітньої діяльності

Перелік літератури

1. Стратегія розвитку вищої освіти в Україні на 2022–2032 роки [Електронний ресурс] : схвалена розпорядженням Кабінету Міністрів України № 286-р від 23 лютого 2022 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/286-2022-p#Text>.

2. Концепція трансформації системи військової освіти [Електронний ресурс] : затверджена постановою Кабінету Ми-

ністрів України № 1410 від 15 грудня 1997 р.: у редакції постанови Кабінету Міністрів України № 1490 від 30 грудня 2022 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/1490-2022-p#Text>.

3. Про освіту [Електронний ресурс] : Закон України № 2145-VIII від 5 вересня 2017 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/2145-19#Text>.

4. Про вищу освіту [Електронний ресурс] : Закон України № 1556-VII від 1 липня 2014 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/1556-18#Text>.

5. Вітченко А. О. Розвиток системи вищої військової освіти України в контексті сучасних трансформаційних змін [Електронний ресурс] / А. О. Вітченко, В. І. Осьодло // Наука і оборона. – 2019. – № 2. – С. 44–50. – Режим доступу : <https://doi.org/10.33099/2618-1614-2019-7-2-44-50>.

6. Зельницький А. Якість вищої військової освіти в контексті змін у законодавстві України [Електронний ресурс] / А. Зельницький, О. Заболотний // Військова освіта : зб. наук. праць. – 2020. – № 1 (41). – С. 147–162. – Режим доступу : <https://doi.org/10.33099/2617-1783/2020-1/147-162>.

7. Harvey L. Defining quality [Електронний ресурс] / L. Harvey, D. Green // Assessment & Evaluation in Higher Education. – 1993. – Vol. 18, issue 1. – P. 9–34. – Режим доступу : <https://doi.org/10.1080/0260293930180102>.

8. Parri J. Quality in Higher Education / J. Parri // Vadyba = Management. – 2006. – № 2 (11). – P. 107–111.

9. Організаційно-методичні рекомендації щодо гарантування якості вищої військової освіти у вищих військових навчальних закладах та військових навчальних підрозділах закладів вищої освіти / А. М. Зельницький, О. А. Заболотний, О. М. Васильєв та ін. – К. : НУОУ ім. І. Черняховського. – 2020. – 120 с.

10. Інноваційні педагогічні технології та методики в освітньому процесі військових навчальних закладів провідних країн – членів НАТО і України : колектив. моногр. / [В. С. Рижиков та ін.]; за заг. ред. В. С. Рижикова ; Військ. ін-т Київ. нац. ун-ту ім. Тараса Шевченка. – К. : Ямчинський О. В. [вид.], 2020. – 341 с.

11. Вітченко А. О. Технології навчання у вищій військовій школі: теорія і практика : навч.-метод. посіб. / А. О. Вітченко, В. І. Осьодло, С. М. Салкуцян ; за заг. ред. В. М. Телелима. – К. : НУОУ ім. І. Черняховського, 2016. – 271 с.

12. Зельницький А. Технологізація освітнього процесу вищих військових навчальних закладів [Електронний ресурс] / А. Зельницький, О. Заболотний, Л. Левицька // Військова освіта : зб. наук. праць. – 2018. – № 1 (37). – С. 114–124. – Режим доступу : <https://doi.org/10.33099/2617-1783/2018-1/114-124>.

13. Modernizing Learning: Building the Future Learning Ecosystem / editors J. J. Walcutt, S. Schatz ; Advanced Distributed Learning (ADL) Initiative. – Washington, DC : Government Publishing Office, 2019. – 416 p.

14. Теоретико-методологічні засади управління змінами в системі військової освіти : монографія / А. М. Зельницький, О. А. Заболотний, О. М. Васильєв, Н. О. Шабатіна ; НУОУ ім. І. Черняховського. – К. : НУОУ ім. І. Черняховського, 2022. – 312 с.

DOI 10.33099/2618-1614-2023-23-4-23-28
УДК [629.7.025.1::629.735.33]:533.6.013.422

О. В. Сафронов,

доктор технічних наук, професор, провідний науковий співробітник центру воєнно-стратегічних досліджень, Національний університет оборони України,

Б. Й. Семон,

доктор технічних наук, професор, головний науковий співробітник науково-методичного центру організації наукової та науково-технічної діяльності, Національний університет оборони України,

О. М. Неділько,

кандидат технічних наук, доцент, провідний науковий співробітник науково-методичного центру організації наукової та науково-технічної діяльності, Національний університет оборони України

Метод оцінювання максимального рівня коливань аеродинамічних поверхонь керування надзвукових літаків у разі виникнення трансзвукового флатера

У статті запропонований метод оцінювання максимального рівня коливань аеродинамічних поверхонь керування надзвукових літаків у разі виникнення трансзвукового флатера, згідно з яким рівень коливань поверхонь керування визначається з умови порівняння їхніх збуджених шарнірних моментів і шарнірних моментів від сил аеродинамічного та конструкційного демпфірування. Метод може бути рекомендований для попереднього наближеного оцінювання максимального рівня коливань аеродинамічних поверхонь керування під час досліджень трансзвукового флатера. Можливість використання запропонованого методу оцінювання максимального рівня коливань аеродинамічних поверхонь керування підтверджена шляхом порівняння результатів розрахунків, одержаних за допомогою цього методу, з результатами, одержаними в експериментальних дослідженнях.

Ключові слова: математична модель, коливання, аеродинамічна поверхня керування, надзвукові літаки, безпека, число M польоту, трансзвуковий флатер, максимальний рівень коливань.

© О. В. Сафронов, Б. Й. Семон, О. М. Неділько, 2023

Постановка проблеми. Визначення безпечного рівня коливань аеродинамічних поверхонь керування надзвукових літаків у льотних дослідженнях трансзвукового флатера теоретичними методами залишається актуальною науковою та прикладною проблемою, оскільки оцінювання цього явища прямими методами, тобто шляхом досягнення максимально можливих режимів польоту безпосередньо в льотних дослідженнях, небезпечна.

Аналіз основних досліджень і публікацій. Теоретичним та експериментальним методам дослідження цього явища присвячено чимало публікацій [1–8], у яких запропоновані різноманітні підходи до обґрунтування причин виникнення інтенсивних коливань аеродинамічних поверхонь керування надзвукових літаків.

У цих дослідженнях відзначений нелінійний характер коливань та їхня залежність від великої кількості різноманітних параметрів [2]. До можливих причин виникнення коливань віднесена різна інтенсивність стрибків ущільнення під час їх переміщення вперед і назад по профілю поверхні керування [3], фазові відношення між коливаннями поверхонь керування та рухом стрибків ущільнення [4], складна взаємодія стрибків ущільнення з коливаннями поверхонь керування [5–8]. Але справжній механізм цих коливань залишається остаточно не з'ясованим [2].

Одна з можливих математичних моделей цього явища запропонована в роботі [5] у вигляді диференційного рівняння другого порядку з нелінійною правою частиною

$$\ddot{\delta}(t) + \frac{\nu}{\pi} \omega \dot{\delta}(t) + \omega^2 \delta(t) = \frac{1}{J_k} [\bar{M}_a(\dot{\delta}) + \bar{M}_c(\dot{\delta})], \quad (1)$$

де $\delta(t)$ – характер коливань аеродинамічної поверхні керування;

ν – логарифмічний декремент коливань поверхні керування;

ω – кутова частота власних пружних коливань поверхні керування;

J_k – розподілений масовий момент інерції поверхні керування;

$\bar{M}_a(\dot{\delta})$ – розподілений шарнірний момент поверхні керування, зумовлений силами аеродинамічного демпфірування;

$\bar{M}_c(\dot{\delta})$ – розподілений збуджений шарнірний момент, зумовлений взаємодією коливань стрибків ущільнення з коливаннями поверхонь керування.

До цих шарнірних моментів аеродинамічної поверхні керування слід віднести і момент, зумовлений силами конструкційного демпфірування та інерційними характеристиками поверхні керування. Розподілена величина цього моменту, як випливає з рівняння (1), дорівнює

$$\bar{M}_k(\dot{\delta}) = -\frac{1}{\pi} J_k \nu \omega \dot{\delta}(t). \quad (2)$$

Мета статті – обґрунтувати можливість оцінювання максимального рівня коливань аеродинамічних поверхонь керування надзвукових літаків у разі виникнення трансзвукового флатера шляхом порівняння збуджених шарнірних моментів аеродинамічних поверхонь керування і шарнірних моментів від сил аеродинамічного та конструкційного демпфірування.

Виклад основного матеріалу. Найбільші труднощі у розв’язанні рівняння (1) виникають саме під час визначення збудженого шарнірного моменту аеродинамічної поверхні керування. У роботі [7] була запропонована математична модель оцінювання величини збудженого шарнірного моменту, тобто моменту, внаслідок якого виникають коливання аеродинамічних поверхонь керування. Розподілена величина цього моменту визначається рівнянням

$$\overline{M}_c(\dot{\delta}) \approx \Delta P_0 \left[1 - \frac{1}{2} \frac{b_k}{\varphi_0 V_\phi} |\dot{\delta}(t)| \right] \frac{b_k^2 \dot{\delta}(t)}{\varphi_0 V_\phi \left[1 + \frac{b_1}{\varphi_0 V_\phi} |\dot{\delta}(t)| \right]^2}, \quad (3)$$

де ΔP_0 – максимальна величина зміни тиску місцевого надзвукового струменя за умови розташування стрибків ущільнення на задній кромці поверхні керування та за умови відсутності коливань;

b_k – хорда профілю поверхні керування;

φ_0 – максимальний кут нахилу дотичної до дифузornoї частини профілю за умови відсутності коливань поверхні керування;

V_ϕ – швидкість польоту літака, за якої виникають коливання аеродинамічних поверхонь керування;

b_1 – відстань лінії максимальної товщини профілю від його задньої кромки.

Оскільки математична модель оцінювання величини збудженого шарнірного моменту поверхні керування має нелінійний характер, то розв’язок диференційного рівняння (1), тобто визначення амплітуди коливань поверхні керування в разі виникнення трансзвукового флатера, можна одержати за допомогою методу енергетичного балансу [9].

Згідно з методом енергетичного балансу амплітуда коливань аеродинамічних поверхонь керування визначається з рівності робіт збудженого шарнірного моменту аеродинамічних поверхонь керування і шарнірних моментів від сил аеродинамічного та конструкційного демпфірування за один період коливань.

Оскільки інтеграл залежності (3) не є табличним, у роботі [6] ця залежність була визначена адаптованою математичною моделлю збудженого шарнірного моменту аеродинамічних поверхонь керування, згідно з якою в роботі [8] і була визначена амплітуда цих коливань у разі виникнення трансзвукового флатера.

Але слід зауважити, що в тій самій роботі [6] визначена і максимально можлива величина розподіленого збудженого шарнірного моменту аеродинамічних поверх-

онь керування надзвукових літаків у разі виникнення трансзвукового флатера, подана залежністю

$$\overline{M}_0(\dot{\delta}) \approx 0,5 P_n (M_{10} - M_\infty) \frac{b_1 b_k^2}{2b_1 + b_k}, \quad (4)$$

де P_n – тиск повітря на висоті польоту;

M_{10} – максимальне число M місцевого надзвукового струменя на поверхні керування за умови розташування стрибків ущільнення на задній кромці профілю та за умови відсутності коливань;

M_∞ – число M незбудженого потоку повітря за умови розташування стрибків ущільнення на задній кромці профілю та за умови відсутності коливань.

Максимальна можлива величина цього шарнірного моменту спостерігається за умови

$$\dot{z}(t) = \frac{b_1}{b_1 + b_k}, \quad (5)$$

де $\dot{z}(t)$ – груповий безрозмірний параметр, який ураховує геометричні дані аеродинамічного профілю, умови польоту літака й характер коливань аеродинамічної поверхні керування і визначається залежністю

$$\dot{z}(t) = \frac{b_1}{\varphi_0 V} \dot{\delta}(t). \quad (6)$$

Відомо [1–4], що коливання аеродинамічних поверхонь керування в разі виникнення трансзвукового флатера близькі до гармонічних коливань, тобто

$$\delta(t) = \delta_0 \sin \omega t, \quad (7)$$

де δ_0 – амплітуда коливань аеродинамічної поверхні керування.

З рівнянь (5)–(7) одержуємо мінімальну амплітуду коливань аеродинамічної поверхні керування, за якої збуджений шарнірний момент досягає максимальної величини й можливе виникнення трансзвукового флатера

$$\delta_{0\phi} = \frac{\varphi_0 V_\phi}{\omega(b_1 + b_k)}, \quad (8)$$

де $\delta_{0\phi}$ – мінімальна амплітуда коливань аеродинамічної поверхні керування, за якої збуджений шарнірний момент досягає максимальної величини й можливе виникнення трансзвукового флатера.

Зауважимо, що амплітуда коливань аеродинамічних поверхонь керування сучасних надзвукових літаків, за якої збуджений шарнірний момент досягає максимальної величини й можливе виникнення трансзвукового флатера, спостерігається за умови

$$\delta_{0\phi} \approx 0,5 \varphi_0. \quad (9)$$

З умови (9) слідує, що збуджений шарнірний момент у разі виникнення трансзвукового флатера досягає максимальної величини за невеликих амплітуд коливань аеродинамічних поверхонь керування.

З аналізу залежності (4) випливає, що максимальна можлива величина збудженого шарнірного моменту

аеродинамічної поверхні керування залежить лише від умов польоту і геометричних характеристик системи «крило – аеродинамічна поверхня керування».

Зауважимо також, що коли амплітуди коливань аеродинамічної поверхні керування перевищують величину, визначену умовою (9), максимально можлива величина збудженого шарнірного моменту незначно зменшується. Тобто спостерігається ефект стабілізації збуджених шарнірних моментів аеродинамічних поверхонь керування.

Але, як можна бачити з рівняння (2), залежність шарнірного моменту від сил конструкційного демпфірування лінійно зростає зі збільшенням амплітуди коливань аеродинамічної поверхні керування.

Також зі збільшенням амплітуди коливань аеродинамічної поверхні керування лінійно зростає і величина шарнірного моменту від сил аеродинамічного демпфірування. Розподілена величина цього шарнірного моменту поверхні керування у праці [1] визначена залежністю

$$\bar{M}_a(\dot{\delta}) \approx -\frac{3}{8} \pi \rho_H V_\phi b_k^3 \dot{\delta}(t), \quad (10)$$

де ρ_H – густина повітря на висоті польоту.

З наведеного випливає, що максимальний рівень коливань аеродинамічної поверхні керування в разі виникнення трансзвукового флатера можна одержати спрощеним методом, без перетворення залежності (3), а саме шляхом порівняння збудженого шарнірного моменту, який визначається залежністю (4), і шарнірних моментів від сил аеродинамічного та конструкційного демпфірування, які визначаються залежностями (2) і (10).

З метою підвищення точності оцінювання рівня коливань аеродинамічної поверхні керування в разі виникнення трансзвукового флатера величину шарнірного моменту (10) визначимо за допомогою гіпотези динамічного скривлення [10], згідно з якою аеродинамічні характеристики профілю, що коливається, не відрізняються від характеристик сталого профілю, скривленого таким чином, що зміни місцевих (динамічних) кутів атаки його обтікання потоком повітря повинні відповідати умові

$$\Delta\delta(x; t) = \frac{x}{V_\phi} \dot{\delta}(t), \quad (11)$$

де x – відстань перетину хорди профілю поверхні керування від осі її обертання.

Відомо [1, 10], що складова розподіленої підйімальної сили, зумовлена кутом атаки, у тому числі й динамічним кутом (11), визначається залежністю

$$\Delta\bar{F}_1(x; \dot{\delta}) = C_y^\delta q \Delta\delta(x; t) = C_y^\delta \frac{q}{V_\phi} x \dot{\delta}(t), \quad (12)$$

де C_y^δ – похідна коефіцієнту підйімальної сили за кутом відхилення поверхні керування;

q – швидкісний напір незбудженого потоку повітря.

Розподілений шарнірний момент поверхні керування, зумовлений цією складовою підйімальної сили, визначається інтегралом від залежності (12)

$$\Delta\bar{M}_1(x; \dot{\delta}) = -\int_0^{b_k} \Delta\bar{F}_1(x; \dot{\delta}) dx. \quad (13)$$

Підставляючи залежність (12) в інтеграл (13), одержуємо максимальну величину цього шарнірного моменту поверхні керування

$$\Delta\bar{M}_1(\dot{\delta}) = -\frac{1}{3} C_y^\delta \frac{q}{V_\phi} b_k^3 \dot{\delta}(t). \quad (14)$$

Крім складової підйімальної сили, зумовленої динамічним кутом атаки, на профіль діє аеродинамічна сила, зумовлена динамічною кривизною аеродинамічного профілю поверхні керування. Величину цієї складової розподіленої підйімальної сили визначимо за допомогою наближеної формули С. А. Чаплигіна [11]

$$\Delta\bar{F}_2(f) \approx 2C_{y\phi}^\delta q f_0, \quad (15)$$

де f_0 – максимальна величина кривизни профілю поверхні керування.

Можливість використання цієї формули для визначення аеродинамічної підйімальної сили, зумовленої динамічною кривизною профілю, була доведена в роботі [12].

Характер динамічного скривлення профілю поверхні керування визначається інтегралом від динамічного кута, поданого залежністю (11)

$$f(x; \dot{\delta}) = \int \frac{x}{V_\phi} \dot{\delta}(t) dx = \frac{1}{2} \frac{x^2}{V_\phi} \dot{\delta}(t). \quad (16)$$

Максимальною величина динамічного скривлення буде при $x = 0,5b_k$ і, як випливає з рівняння (16), дорівнюватиме

$$f_0(\dot{\delta}) = \frac{1}{8} \frac{b_k^2}{V_\phi} \dot{\delta}(t). \quad (17)$$

Центр тиску цієї складової підйімальної сили розташований у середині хорди профілю поверхні керування. З урахуванням цього зауваження та залежностей (15) і (17) складову шарнірного моменту поверхні керування, зумовлену динамічною кривизною профілю поверхні керування, можна подати у вигляді

$$\Delta\bar{M}_2(f; \dot{\delta}) \approx -\frac{1}{8} C_{y\phi}^\delta \frac{q}{V_\phi} b_k^3 \dot{\delta}(t). \quad (18)$$

Таким чином, розподілений шарнірний момент поверхні керування, зумовлений силами аеродинамічного демпфірування, визначається сумою залежностей (14) та (18) і дорівнює

$$\bar{M}_a(\dot{\delta}) \approx -0,458 C_y^\delta \frac{q}{V_\phi} b_k^3 \dot{\delta}(t). \quad (19)$$

Ураховуючи наведене вище та беручи до уваги, що в разі виникнення трансзвукового флатера коливання аеродинамічних поверхонь керування мають гармонічний характер, максимальну амплітуду коливань визначимо з рівності залежностей (2), (4) та (19):

$$\delta_0 = \frac{0,5P_H(M_{10} - M_\infty) \frac{b_1 b_k^2}{2b_1 + b_k}}{0,458C_y^a \frac{q}{V_\phi} b_k^3 \omega + \frac{1}{\pi} \bar{J}_k \nu \omega^2} . \quad (20)$$

Максимальне число M_{10} у рівнянні (20) визначається відомою наближеною залежністю [7]

$$M_{10} \approx \sqrt[3]{1 + 11,5 \varphi_0} . \quad (21)$$

Число M_∞ незбудженого потоку повітря в рівнянні (20) визначається з умови формування стрибків ущільнення на поверхні аеродинамічного профілю [5, 7]

$$M_{10} - 1 \approx 2(M_\infty - M_{кр}) , \quad (22)$$

де $M_{кр}$ – критичне число M аеродинамічного профілю.

Критичне число M аеродинамічного профілю в рівнянні (22) може бути визначене за результатами лабораторних досліджень [4, 13] або з такої наближеної залежності [5]:

$$M_{кр} \approx 1 - 0,7 \sqrt{\bar{\tau} \cos \chi} , \quad (23)$$

де $\bar{\tau}$ – відносна товщина аеродинамічного профілю;
 χ – кут стрілоподібності аеродинамічного профілю.

З метою визначення максимальної амплітуди коливань аеродинамічної поверхні керування в разі виникнення трансзвукового флатера, нагадаємо відомі залежності [14]:

$$q = \frac{1}{2} \rho_H V_\phi^2 = \frac{1}{2} k M_\phi^2 P_H ; \quad (24)$$

$$V_\phi = a_H M_\phi , \quad (25)$$

де k – показник адіабати (для повітря $k \approx 1,405$),
 M_ϕ – число M незбудженого потоку повітря, при якому виникає трансзвуковий флатер;
 a_H – швидкість звуку на висоті польоту.

З урахуванням залежностей (24) та (25) залежність (20) може бути подана у вигляді

$$\delta_0 = \frac{0,5P_H(M_{10} - M_\infty) \frac{b_1 b_k^2}{2b_1 + b_k}}{0,458\pi \rho_H a_H M_\phi \omega b_k^3 + \frac{1}{\pi} \bar{J}_k \nu \omega^2} . \quad (26)$$

У залежностях (25) і (26) невідоме число M_ϕ можна визначити з умови формування стрибків ущільнення (22), яке в даному випадку має вигляд

$$M_{1\phi} - 1 \approx 2(M_\phi - M_{кр}) , \quad (26)$$

де $M_{1\phi}$ – число M місцевого надзвукового струменя на поверхні керування, за якого виникає трансзвуковий флатер.

Число $M_{1\phi}$ може бути визначене залежністю, аналогічною до залежності (21), але слід зауважити таке.

Під час коливань поверхні керування максимальний кут обтікання профілю φ_0 місцевим надзвуковим струменем зменшується на величину

$$\Delta\varphi(\dot{\delta}) = \frac{b_k}{V_\phi} \dot{\delta}(t) . \quad (28)$$

У роботі [6] доведено, що максимальна величина збудженого шарнірного моменту поверхні керування спостерігається за умови

$$\frac{b_1}{\varphi_0 V_\phi} \dot{\delta}(t) = \frac{b_1}{b_1 + b_k} . \quad (29)$$

Із сумісного розв'язання залежностей (28) і (29) одержимо

$$\Delta\varphi(\dot{\delta}) = \varphi_0 \frac{b_k}{b_1 + b_k} . \quad (30)$$

З урахуванням залежностей (21) і (30) число $M_{1\phi}$ визначимо таким чином:

$$M_{1\phi} \approx \sqrt[3]{1 + 11,5(\varphi_0 - \Delta\varphi)} = \sqrt[3]{1 + 11,5 \frac{b_1}{b_1 + b_k} \varphi_0} . \quad (31)$$

Можливість визначення максимальної амплітуди коливань аеродинамічних поверхонь керування в разі виникнення трансзвукового флатера теоретичним методом оцінимо шляхом порівняння результатів, одержаних за допомогою рівняння (26) і результатів, одержаних у льотних дослідженнях.

Максимальну амплітуду коливань аеродинамічних поверхонь керування в разі виникнення трансзвукового флатера визначимо з рівняння (26) за таких вхідних даних:

а) характеристики аеродинамічного профілю:

- відстань лінії максимальної товщини аеродинамічного профілю від його задньої кромки – $b_1 = 1,5$ м;

- відносна товщина аеродинамічного профілю – $\bar{\tau} = 0,042$;

- кут стрілоподібності – $\chi = 45^\circ$;

б) характеристики поверхні керування:

- середня аеродинамічна хорда – $b_k = 0,75$ м.;

- розподілений масовий момент інерції – $\bar{J}_k = 1,0$ Н сек²;

- логарифмічний декремент коливань поверхні керування – $\nu = 0,7$;

- кутова частота власних коливань – $\omega = 239$ рад./сек.;

- похідна коефіцієнта піднімальної сили аеродинамічної поверхні керування літака за кутом її відхилення [14] – $C_y^\delta = 2\pi$;

- максимальний кут нахилу дотичної до профілю поверхні керування для типових профілів ЦАГІ [8] – $\varphi_0 \approx 0,85$ $\bar{\tau} = 0,0357$ рад.

Розрахункові дані для визначення амплітуди коливань аеродинамічних поверхонь керування:

- максимальне число M місцевого надзвукового струменя на поверхні керування за умови розташування стрибків ущільнення на задній кромці профілю – $M_{10} = 1,121$ (згідно з рівнянням (21));

- критичне число M профілю – $M_{кр} = 0,8794$ (згідно з рівнянням (23));

- число M незбудженого потоку повітря за умови розташування стрибків ущільнення на задній кромці профілю – $M_{\infty} = 0,94$ (згідно з рівнянням (22));

- число M місцевого надзвукового струму на поверхні керування, за якого виникає трансзвуковий флатер – $M_{1ф} = 1,084$ (згідно з рівнянням (31));

- число M незбудженого потоку повітря, за якого виникає трансзвуковий флатер – $M_{ф} = 0,9214$ (згідно з рівнянням (27)).

Умови виконання льотного експерименту і рівень коливань аеродинамічної поверхні керування за стандартних величин швидкості звуку і густини повітря на висоті польоту $H = 0$ км [15]:

- швидкість польоту, за якої виникає трансзвуковий флатер – $V_{ф} = 313,46$ м/с (згідно з рівнянням (25) при $M_{ф} = 0,9214$);

- рівень коливань поверхні керування $\delta_0 = 1,49^\circ$.

Підставляючи ці дані і стандартні величини швидкості звуку й густини повітря в рівняння (26), одержимо максимально можливу величину амплітуди коливань аеродинамічної поверхні керування в разі виникнення трансзвукового флатера

$$\delta_0 = 0,0302 \text{ рад.} = 1,73^\circ.$$

Зауважимо, що одержана максимально можлива величина амплітуди коливань аеродинамічної поверхні керування на 16% більше, ніж у льотному експерименті.

Цю розбіжність можна пояснити таким чином.

З аналізу рівнянь (2) та (26) бачимо, що величина шарнірного моменту аеродинамічної поверхні керування визначена силами конструкційного демпфірування та інерційними характеристиками поверхні керування. У реальних умовах цей шарнірний момент залежить від характеристик системи «привод – аеродинамічна поверхня керування», а не лише від характеристик поверхні керування. Як вказано в роботі [8], визначення цих характеристик у лабораторних дослідженнях пов'язане з великими труднощами, оскільки практично неможливо відокремити частки шарнірних моментів, зумовлені аеродинамічними силами, силами конструкційного демпфірування та інерційними характеристиками системи «привод – аеродинамічна поверхня керування». Тому рівень коливань поверхні керування, одержаний за допомогою розрахункового методу, завжди більший, ніж рівень коливань, одержаний у льотному експерименті.

Утім, більший, а не менший. І це йде у запас міцності елементів конструкції поверхні керування, а тому й у запас безпеки польотів надзвукових літаків на трансзвукових швидкостях.

Цей метод може бути рекомендований для попереднього наближеного оцінювання максимального рівня коливань аеродинамічних поверхонь керування в перших випробувальних польотах надзвукових літаків під час досліджень характеристик трансзвукового флатера.

Прогнозування рівня коливань аеродинамічних поверхонь керування надзвукових літаків в експериментальних дослідженнях трансзвукового флатера доцільно виконувати за допомогою розрахунково-експериментального методу, як це було рекомендовано в роботі [8].

Висновки. У статті запропонований метод оцінювання максимального рівня коливань аеродинамічних поверхонь керування надзвукових літаків у разі виникнення трансзвукового флатера, згідно з яким рівень коливань аеродинамічних поверхонь керування визначається з умови порівняння їхніх максимально можливих збуджених шарнірних моментів і шарнірних моментів від сил аеродинамічного та конструкційного демпфірування.

Можливість використання запропонованого методу для попереднього наближеного оцінювання максимального рівня коливань аеродинамічних поверхонь керування підтверджена шляхом порівняння результатів розрахунків, одержаних за допомогою цього методу, з результатами, одержаними в експериментальних дослідженнях.

Подальші дослідження доцільно присвятити аналізу методів зменшення коливань аеродинамічних поверхонь керування в разі виникнення трансзвукового флатера.

Перелік літератури

1. Бисплингхофф Р. Л. Аэроупругость / Р. Л. Бисплингхофф, Х. Эшли, Р. Л. Халфмэн ; пер. с англ. Г. И. Баренблатта, А. И. Смирнова, В. П. Шидловского ; под ред. Э. И. Григолюка. – М. : Изд-во иностран. лит., 1958. – 800 с.
2. Аэродинамическое исследование колеблющейся поверхности управления при трансзвуковых скоростях / ЦАГИ. – М. : ЦАГИ, 1975. – 105 с. – (Обзоры ЦАГИ ; № 456).
3. Агеев Ю. И. Экспериментальное исследование установившихся колебаний элерона в околосзвуковом потоке / Ю. И. Агеев, В. В. Назаренко, Т. П. Небезина // Ученые записки ЦАГИ. – 1974. – Том V, № 8. – С. 71–80.
4. Левкин В. Ф. Экспериментальные исследования нестационарных аэродинамических характеристик поверхностей управления при трансзвуковых скоростях / В. Ф. Левкин. – М. : ЦАГИ, 1982. – 16 с. – (Труды ЦАГИ ; выпуск 2132).
5. Сафронов А. В. Уровень автоколебаний аэродинамических поверхностей управления при безотрывном обтекании околосзвуковым потоком газа / А. В. Сафронов // Проблемы прочности. – 1991. – № 4. – С. 51–55.
6. Сафронов О. В. Адаптована математична модель оцінки збуджених шарнірних моментів аеродинамічних поверхонь керування надзвукових літаків на трансзвукових швидкостях польоту / О. В. Сафронов, О. М. Неділько, В. О. Сафронов // Збірник наукових праць ЦВСД НУОУ ім. І. Черняхівського. – 2014. – № 3 (52). – С. 28–33.
7. Сафронов А. В. Аэродинамическое воздействие скачков уплотнения на колеблющийся в околосзвуковом потоке элерон / А. В. Сафронов // Ученые записки ЦАГИ. – 1991. – Том XXII, № 3. – С. 110–117.

8. Сафронов О. В. Порівняльний аналіз теоретичних та розрахунково-експериментальних методів оцінки характеристик трансзвукового флатера / О. В. Сафронов, О. М. Неділько, В. О. Сафронов // Збірник наукових праць ЦВСД НУОУ ім. І. Черняхівського. – 2015. – № 1 (53). – С. 41–48.

9. Пановко Я. Г. Введение в теорию механических колебаний / Я. Г. Пановко. – М. : Наука, 1980. – 272 с.

10. Келдыш М. В. Избранные труды. Механика / пред. ред. кол. А. П. Александров. – М. : Наука, 1985. – 568 с.

11. Чаплыгин С. А. О давлении плоскопараллельного потока на преграждающие тела // Избранные труды. Механика жидкости и газа. Математика. Общая механика / пред. ред. кол. А. П. Виноградов. – М. : Наука, 1976. – (Классики науки). – С. 97–130.

12. Сафронов А. В. Применение формулы Чаплыгина С. А. для оценки аэродинамической силы колеблющегося профиля / А. В. Сафронов // Научно-технический сборник КВВАИУ. – 1989. – № 7. – С. 57–62.

13. Свищев Г. П. Эффективность руля и шарнирные моменты его при больших скоростях / Г. П. Свищев. – М. : ЦАГИ, 1975. – 10 с. – (Труды ЦАГИ ; выпуск 1722).

14. Гошек И. Аэродинамика больших скоростей / И. Гошек ; пер. с чешского А. А. Дородницына, М. М. Богословского. – М. : Изд-во иностран. лит., 1954. – 547 с.

15. Лебедев А. А. Динамика полета беспилотных летательных аппаратов / А. А. Лебедев, Л. С. Чернобровкин ; под ред. А. А. Лебедева. – М. : Оборонгиз, 1962. – 548 с.

DOI 10.33099/2618-1614-2023-23-4-29-40

УДК 355.4:004.8

С. В. Свешніков,*кандидат технічних наук,
старший науковий співробітник,
провідний науковий співробітник центру
воєнно-стратегічних досліджень,
Національний університет оборони України,***В. П. Бочарніков,***доктор технічних наук, професор,
головний науковий співробітник центру
воєнно-стратегічних досліджень,
Національний університет оборони України*

Використання методів штучного інтелекту для розв'язання наукових задач у сфері оборони

У статті автори на рівні концептуальних моделей демонструють можливості застосування методів штучного інтелекту для розв'язання прикладних наукових задач, які постають у сфері безпеки та оборони.

Ключові слова: штучний інтелект, нечіткі множини, нечіткі міри, нейронні мережі, оцінювання, класифікація, кластеризація, прогнозування.

Унаслідок швидкого поширення інформаційних технологій значно ускладнюються взаємозв'язки між об'єктами реального світу, зокрема ті, що стосуються сфери оборони в широкому розумінні. Поведінка об'єктів стає складнішою та непередбачуванішою. Потреба вивчення взаємозв'язків між об'єктами лише зростає й ускладнюється. На цьому тлі стає дедалі важче забезпечити адекватність наукових рекомендацій за допомогою добре відомих та відпрацьованих методів досліджень. Тому сьогодні рельєфніше проявляється суперечність між спроможностями відомих методів, таких як дослідження операцій, і властивостями сучасних досліджуваних систем та об'єктів. Оскільки ускладнення останніх є об'єктивною та неминучою реальністю, висновок єдиний – це розробка й апробація нових наукових методів і технік, зокрема методів штучного інтелекту, застосування яких останнім часом поширюється для вирішення наукових завдань у різних сферах.

Досвід спілкування в середовищі науковців свідчить, що сьогодні має місце певна недооцінка й навіть нерозуміння спроможностей методів штучного інтелекту з вирішення наукових завдань у сфері оборони. Тому в цій статті автори **мають на меті** на рівні концептуальних моделей продемонструвати можливість розв'язання прикладних наукових задач, які постають у сфері безпеки та оборони, методами штучного інтелекту. Звісно, кількість таких задач досить велика, і показати навіть логіку розв'язання їх усіх у межах статті неможливо. Тому далі використаний такий спосіб розкриття питання: спочатку буде продемонстровано, що більшість наукових задач, у тому числі у сфері оборони, можна типізувати, тобто привести до невеликої кількості формальних типів задач, а потім будуть наведені деякі техніки розв'язання типових наукових задач методами штучного інтелекту.

Одразу зазначимо, що єдиного визначення терміна «штучний інтелект» не існує. Але більшість людей розуміють штучний інтелект як науковий напрям і технологію створення інтелектуальних систем, тобто систем, спроможних розв'язувати насамперед складні задачі подібно до того, як їх розв'язує людина, а саме застосовуючи «м'які, не визначені точно» дані й відповідні методи одержання результату, зокрема навчання. Класифікація цих методів також не є загальноприйнятою. Одним з її варіантів може бути така: нечітка логіка (нечіткі множини, нечіткі міри), нейронні мережі, засновані на знаннях системи (експертні системи), еволюційне моделювання (генетичні алгоритми, багатоагентні системи), методи «BigData» (вивчення великих обсягів даних, пошук невідомих раніше закономірностей).

Звичайно, методів штучного інтелекту на сьогодні існує безліч, та охопити їх у рамках однієї статті неможливо. Тому далі розглядаються найпоширеніші, перевірені на практиці методи.

Типізація наукових задач у сфері оборони

Виходячи з того, що кількість наукових задач у сфері оборони є практично неосяжною, поділимо їх за ознакою характеру досліджуваних у задачах об'єктів, як показано в *таблиці 1*. Цей поділ є досить умовним, але він охоплює більшу частину наукових задач.

Таблиця 1

Поділ наукових задач за характером досліджуваних об'єктів

Група наукових задач	Характер досліджуваних об'єктів
Задачі воєнно-політичного аналізу (безпекові задачі)	Держави та інші воєнно-політичні сили
Задачі стратегічного рівня	Збройні сили, великі стратегічні угруповання
Задачі оперативного рівня	Оперативні угруповання
Задачі тактичного рівня	Військові підрозділи, частини та з'єднання
Задачі інформаційно-психологічних впливів та кібербезпеки	Людина, група людей, інформаційно-керуючі системи
Задачі військової техніки та озброєння	Технічні пристрої
Задачі оборонного планування	Збройні сили, їхні спроможності

Розглянемо далі кілька прикладів наукових задач із кожної групи і надамо їхню коротку характеристику відповідно до класифікації [1] аналітичних задач. Частина наукових задач у прямій постановці сформульована в роботі авторів [1]. Інші наукові задачі сформульовані як такі, що випливають з аналізу наукових праць, опублікованих у провідному відкритому виданні – збірнику наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України. Найчастіше в цих працях представлено або науково-методичний підхід, або концептуальну модель розв'язання наукових задач. Кількісні рішення, як правило, представлені не часто. Але далі ми покажемо, як це можна зробити із застосуванням методів штучного інтелекту. У *таблиці 2* представлені приклади наукових задач та їхня коротка характеристика.

Аналіз свідчить, що найпоширенішим типом наукових задач є задачі оцінювання. Крім того, наявні також задачі вибору, класифікації (віднесення до заздалегідь визначених класів), прогнозування, кластеризації, а також чисельних розрахунків. Розглянемо концептуальні схеми розв'язання цих типових наукових задач, а також техніки розв'язання на основі методів штучного інтелекту.

Розв'язання задач оцінювання

Головною загальною метою розв'язання задач оцінювання є розрахунок оцінок альтернатив у термінах корисності або некорисності. Оцінювання альтернатив

Таблиця 2

Приклади наукових задач та їхня коротка характеристика

Наукова задача	Характеристика наукової задачі
Задачі воєнно-політичного аналізу (безпекові задачі)	
Оцінювання альтернативних варіантів національної політики України щодо формування її статусу відносно міжнародного оточення і структур колективної безпеки [2]	Задача оцінювання. Вхідні дані: варіанти національної політики. Результати розв'язання: оцінки варіантів з погляду критеріїв безпеки
Прогнозування конфліктів на основі вивчення великих обсягів даних з багатьох сфер життєдіяльності (національної безпеки) [3]	Задача прогнозування, яка розв'язується як задача кластеризації майбутніх конфліктів. Вхідні дані: всі дані, які можуть бути пов'язані з виникненням воєнних конфліктів. Результати розв'язання: оцінки можливості виникнення воєнного конфлікту між певними державами в майбутньому
Прогнозування напруженості світової та регіональної воєнно-політичної обстановки [1]	Задача прогнозування. Вхідні дані: проблеми міждержавних відносин, параметри воєнної могутності і потенційної агресивності держав. Результати розв'язання: прогноз напруженості воєнно-політичної обстановки
Прогнозування можливості виникнення внутрішнього збройного конфлікту [1]	Задача прогнозування. Вхідні дані: інтереси і цілі соціальних груп, проблеми внутрішніх відносин. Результати розв'язання: прогноз можливості й умов переростання внутрішніх суперечностей у збройний конфлікт

Продовження таблиці 2

Наукова задача	Характеристика наукової задачі
Визначення структури потенційних воєнно-політичних блоків [1]	Задача кластеризації. Вхідні дані: інтереси і цілі держав, позиції держав за проблемами відносин. Результати розв'язання: можливість утворення воєнно-політичних блоків визначеного складу
Класифікація намірів і дій воєнно-політичних союзів та окремих держав [1]	Задача класифікації. Вхідні дані: наміри та дії держав (союзів) та їхні характеристики. Результати розв'язання: можливість відповідності намірів та дій певним визначеним класам
Задачі стратегічного рівня	
Оцінювання спільних спроможностей об'єднаних сил, інтегрованих у декількох доменах [4]	Задача оцінювання. Вхідні дані: параметри спільних спроможностей об'єднаних сил. Результати розв'язання: оцінки відповідності спроможностей вимогам з боку воєнних конфліктів або стосовно заданого рівня спроможностей
Вибір способу дій коаліційних сил спеціальних операцій [5]	Задача вибору. Вхідні дані: множина способів дій коаліційних сил спеціальних операцій та їхні параметри. Результати розв'язання: оцінки способів дій
Задачі оперативного рівня	
Оцінювання відповідності системи управління міжвидового угруповання вимогам з боку багатодомених операцій під час конфлікту високої інтенсивності [6]	Задача оцінювання. Вхідні дані: параметри системи управління та критерії, що відображають вимоги. Результати розв'язання: оцінки рівня відповідності параметрів системи управління критеріям
Оцінювання ефективності дій міжвидового угруповання в багатодомених операціях [6]	Задача оцінювання. Вхідні дані: параметри міжвидового угруповання та їхніх дій. Результати розв'язання: оцінка ефективності дій, умови досягнення заданого рівня ефективності
Задачі тактичного рівня	
Розрахунок кількості та складу мобільних протидиверсійних резервів під час оперативного розгортання військ [7]	Задача чисельних розрахунків. Вхідні дані: характеристики своїх підрозділів та підрозділів противника, оперативної побудови. Результати розв'язання: оцінки кількості та складу мобільних протидиверсійних резервів
Оцінювання рівня зниження ефективності системи управління військами противника в результаті ракетного удару [8]	Задача оцінювання. Вхідні дані: варіанти розподілу засобів ураження за об'єктами системи управління. Результати розв'язання: оцінки рівня зниження ефективності системи управління військами противника за варіантами
Оцінювання можливості досягнення потрібного ефекту координації вогневого ураження противника в операції [9]	Задача оцінювання. Вхідні дані: об'єкти противника, бойовий склад своїх сил, вимоги до ураження об'єктів. Результати розв'язання: найраціональніший варіант розподілу сил та засобів за об'єктами
Задачі інформаційно-психологічних впливів та кібербезпеки	
Оцінювання рівня інформаційно-психологічного впливу противника в інтересах інформаційної операції Збройних Сил України [10]	Задача чисельних розрахунків. Вхідні дані: параметри інформаційно-психологічного впливу. Результати розв'язання: узагальнена оцінка рівня інформаційно-психологічного впливу противника
Оцінювання можливості появи і наслідків реалізації ризику безпеки інформації [11]	Задача оцінювання. Вхідні дані: параметри інформаційної системи, параметри зовнішнього інформаційного середовища. Результати розв'язання: оцінки можливості появи і можливості наслідків реалізації ризиків

Продовження таблиці 2

Наукова задача	Характеристика наукової задачі
Оцінювання захищеності інформаційної інфраструктури за кількома ознаками і показниками [12]	Задача оцінювання. Вхідні дані: параметри інформаційної інфраструктури, критерії оцінювання. Результати розв'язання: оцінка рівня захищеності
Виявлення та прогноз інтенсивності інформаційних впливів на світобачення населення [1]	Задача прогнозування. Вхідні дані: потік інформаційних повідомлень, структура уподобань населення. Результати розв'язання: можливість цілеспрямованого інформаційного впливу
Задачі військової техніки та озброєння	
Вибір варіантів конструкторських рішень щодо побудови автоматизованих систем в інтересах оборони на основі дата-центричного підходу з використанням хмарних технологій [13]	Задача вибору. Вхідні дані: перелік і параметри рішень, критерії оцінювання. Результати розв'язання: оцінки ефективності рішень
Аналіз графіків кардіографічної активності людини для визначення психофізіологічного стану воїнів Сил оборони України за допомогою мініатюрних кардіографічних засобів [14]	Задача оцінювання. Вхідні дані: характеристики графіків. Результати розв'язання: оцінки психофізіологічного стану
Задачі оборонного планування	
Оцінювання рівня корупції в Міністерстві оборони України [15]	Задача оцінювання. Вхідні дані: ознаки корупційних дій. Результати розв'язання: оцінки рівня корупції
Оцінювання спроможностей зенітних ракетних комплексів (ЗРК) щодо оборони військ та об'єктів від ударів нестратегічних балістичних ракет [16]	Задача оцінювання. Вхідні дані: тактико-технічні характеристики ЗРК. Результати розв'язання: оцінки ефективності застосування ЗРК

дає змогу визначити одну або кілька найкращих альтернатив і на цій основі зробити вибір.

Альтернативи описуються кількома параметрами, які можуть мати різну природу. Наприклад, значення параметра можуть завдаватися на безперервній або дискретній множині, вони можуть бути чіткими або нечіткими (розмитими). Як правило, задачі оцінювання є багатокритеріальними, тобто оцінювання відбувається за кількома критеріями. Природа критеріїв також може бути різною. Умовно кажучи, існують два способи розв'язання задач оцінювання: відносний та абсолютний.

Відносний спосіб заснований на порівнянні альтернатив між собою за параметрами з урахуванням важливості параметрів. Цей спосіб реалізований у добре відомому методі аналізу ієрархій Сааті [17]. У зарубіжній науковій літературі цей метод називається «Analytical hierarchy process». Концептуальна схема розв'язання найпростішої задачі оцінювання за допомогою методу аналізу ієрархій наведена на *рисунку 1*.

На *рисунку 1* позначено: c_Σ – головний (узагальнений) критерій оцінювання; $O = \{o_i, i = \overline{1,3}\}$ – множина альтернатив, що оцінюються; $P = \{p_j, j = \overline{1,2}\}$ – множина параметрів альтернатив. Схема алгоритму оцінювання полягає у виконанні послідовних кроків:

1. Альтернативи порівнюються між собою за кожним параметром з P у шкалі переваг, у результаті чого одержують матриці парних порівнянь у вигляді: $M^j = \|m_{kl}^j\|$, де $\forall k, l = \overline{1,3}$, $m_{kl}^j = \pi(o_k \gtrsim o_l) \in L$ – елемент матриці M^j , який визначає перевагу $\gtrsim$ альтернативи o_k над альтернативою o_l у шкалі переваг $\pi(\cdot) \in L$. Для методу аналізу ієрархій Сааті $L = (1,9)$. При цьому якщо $\pi(o_k \gtrsim o_l) = x \in L$, тоді $\pi(o_l \gtrsim o_k) = \frac{1}{x}$, $\pi(o_l \gtrsim o_k) = 1$.

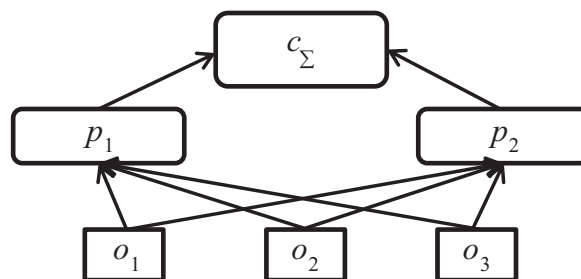


Рис. 1. Концептуальна схема розв'язання задач оцінювання за допомогою методу аналізу ієрархій

2. Одержані матриці M^j об'єднуються в середньозважену матрицю з урахуванням важливості параметрів: $M_\Sigma = \sum_{j=1}^2 b_j M^j$, де b_j – нормована до одиниці вага j -го параметра.

3. Визначається власний вектор $E = \{e_i, i = \overline{1,3}\}$ матриці M_Σ , який відповідає її максимальному власному числу. Власний вектор E містить оцінки узагальненої переваги між альтернативами з множини.

Оскільки на практиці в будь-якій задачі присутня невизначеність, вона має бути врахована в алгоритмі, інакше одержане рішення втрачає адекватність. Сьогодні відомо досить багато напрацювань щодо модернізації методу аналізу ієрархій для врахування нечіткості. Зокрема, середньозважену матрицю можна одержати за допомогою операторів обчислення відстані між двома функціями, наприклад за допомогою дивергенції Кульбака-Лейблера [18] або метрики на декартовому добутку нечітких мір [19]. Іншим варіантом модернізації [20] є використання нечітких аналогів числових оцінок M_{kl}^j , а також ваги b_j . У цьому разі всі перетворення оцінок здійснюються за допомогою алгоритмів нечіткої арифметики [21].

Абсолютний спосіб заснований на порівнянні альтернатив з певним заздалегідь сформованим еталоном (ідеальною альтернативою, яка може бути сформована в явному чи неявному вигляді). Концептуальна схема розв'язання задач оцінювання цим способом наведена на *рисунку 2*, де продемонстрований той самий найпростіший приклад, поданий на *рисунку 1*.

На *рисунку 2* позначено: $Imp = \{Imp_j, j = \overline{1,2}\}$ – множина важливостей критеріїв з $C = \{c_j, j = \overline{1,2}\}$, $Et_j, j = \overline{1,2}$ – еталонні значення параметра p_j , що можуть мати нечіткий характер, $Cur_{i,j}$ – поточне значення параметра p_j альтернативи o_i . Інші позначення такі самі, що й вище. Схема алгоритму оцінювання полягає у виконанні таких кроків:

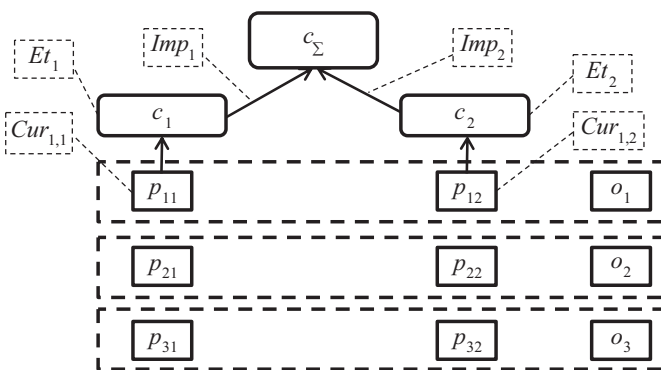


Рис. 2. Концептуальна схема розв'язання найпростішої задачі оцінювання абсолютним способом

1. Визначаються значення важливості Imp_j критеріїв. У загальному випадку ці значення можуть визначатися на основі вимірювань приладами, оброблення статистичних даних або оцінювання експертами.

2. Визначаються еталонні значення Et_j . Ці значення можуть визначатися аналогічно до того, як указано в кроці 1.

3. Визначаються поточні значення параметрів $Cur_{i,j}$ для кожної альтернативи o_i .

4. Для кожної альтернативи o_i поточні значення параметрів $Cur_{i,j}$ послідовно порівнюються з еталонними значеннями Et_j . Порівняння здійснюється за допомогою певного оператора $\simeq$, який у результаті розраховує оцінку відповідності поточного значення еталонному:

$Cor_{i,j} = Cur_{i,j} \simeq Et_j, \forall j = \overline{1,2}$. Вибір виду оператора $\simeq$ має обґрунтовуватися для кожної задачі, виходячи з вимог забезпечення адекватності розрахунків.

5. Для кожної альтернативи o_i оцінки $Cor_{i,j}$ зважуються з урахуванням важливості критеріїв. У результаті розраховується оцінка альтернативи $Est_i = Cor_{i,j} \oplus Imp_j$, де $\oplus$ – позначення оператора зважування. Вибір виду оператора $\oplus$ також має обґрунтовуватися для кожної конкретної задачі. Оцінки Est_i надаються особі, яка приймає рішення.

Звернімо увагу на те, що множину критеріїв, їхні ваги, еталонні значення параметрів альтернатив, а також оператори $\simeq$ та $\oplus$ у сукупності можна розглядати як неявний еталон найкращої альтернативи, оскільки присвоєння оцінкам $Cur_{i,j}$ найкращих значень даватиме найвище значення оцінки альтернативи Est_i . Отже, оцінювання зводиться до порівняння значень параметрів наявних альтернатив з неявним еталоном (ідеальною альтернативою) відповідно до ієрархії критеріїв, рухаючись від критеріїв нижнього рівня до узагальненого критерію. В зарубіжних дослідженнях цю схему часто називають технікою TOPSIS (The Technique for Order of Preference by Similarity to Ideal Solution) [22]. Як бачимо, в цій схемі невизначеність присутня в кількох місцях, зокрема це значення параметрів альтернатив і значення важливості критеріїв оцінювання.

Слід також зазначити, що для коректного розв'язання задач оцінювання і відносним, і абсолютним способами необхідно приділяти максимальну увагу дотриманню таких умов:

- критерії оцінювання мають бути придатними для порівняння між собою, щоб можна було визначити їхні ваги;
- рівень невизначеності початкових даних, потрібних для оцінювання параметрів альтернатив, має давати можливість зробити хоч би приблизне визначення, тобто висунення приблизних припущень стосовно початкових значень параметрів;

- параметри альтернатив можуть бути задані на неперервній чи дискретній множині, числовій або номінальній, за допомогою слів або чисел;

- у разі залежності (взаємодії) критеріїв між собою (внаслідок, як правило, нечіткого формулювання) слід використовувати відповідний математичний апарат або спеціальні методи компенсації систематичних помилок.

Кажучи строго, дотримання цих умов має бути доведене для забезпечення адекватності розв'язання задачі оцінювання.

На сьогодні відомо багато методів реалізації концептуальної схеми розв'язання задачі оцінювання абсолютним способом. Коротко розглянемо їх.

1. Адитивні методи [23], засновані на використанні адитивних мір, зокрема міри ймовірності. Ці методи передбачають визначення Cor_{ij} як відхилення від математичного очікування (Et_j), а також розрахунок Est_i як середньозважених оцінок. Раніше ці методи дуже широко використовувалися.

2. Таксономічні методи [24], засновані на застосуванні різних метричних відстаней, найчастіше відстаней Хеммінга чи Мінковського. У таких методах еталонною оцінкою є точка з $Cor_{ij} = 1, \forall j = \overline{1, 2}$, а оператор $\oplus$ визначає відстань до цієї точки. Залежно від особливостей задачі можуть використовуватися різні типи відстаней [25].

3. Методи штучного інтелекту.

Головним недоліком адитивних і таксономічних методів залишається компенсація одних оцінок іншими, тобто альтернатива може одержати високу оцінку, попри значну кількість параметрів з невисокими оцінками. Це також є причиною невисокої вибірковості методів – у разі, коли альтернативи мають 9–10 параметрів, узагальнена оцінка майже не чутлива до зміни одного з параметрів. Деякі конструкції узагальнення неможливо реалізувати за допомогою цих методів, наприклад логічне «І». Цей перелік недоліків можна продовжити, але їхня природа виходить з невідповідності аксіоматики (властивостей) методів властивостям задач.

На відміну від зазначених методів, методи штучного інтелекту не цілком, але певним чином позбавлені цих недоліків. Вони передбачають опис оцінок та важливості критеріїв за допомогою спеціальних математичних конструкцій, які не вимагають забезпечення умови адитивності оцінок (відстаней). Послаблення аксіоматичного базису завжди додає досліднику новий ступінь свободи і нові можливості. Слід зазначити, що методи штучного інтелекту теж мають складності в застосуванні, пов'язані переважно зі складністю виявлення знань і задавання вхідних оцінок.

На сьогодні існує величезна кількість методів штучного інтелекту. Серед них на практиці найпоширеніші такі.

Методи нечітких множин передбачають, що оцінки альтернатив у критеріях і ваги критеріїв описані

функціями належності нечітких множин, а як оператори порівняння $\simeq$ та узагальнення $\oplus$ використовуються Т-норми та/або Т-конорми [26]. Якщо позначити як $\{Cor_{ij} = 1, \forall j = \overline{1, 2}\}$ множину оцінок альтернативи o_i в критеріях із множини C , то функція належності нечіткої множини оцінок у критеріях може бути описана як: $g_i(c_j): C \rightarrow [0, 1]$. Аналогічно функція належності нечіткої множини вагів критеріїв може бути описана як: $h_i(c_j): C \rightarrow [0, 1]$.

Найпоширенішим випадком оператора узагальнення є оператор максиміну. Наприклад, така операція розраховує узагальнену оцінку альтернативи o_i :

$$o_i: Est_i = \max_j \min (Cor_{ij}, Imp_j) .$$

Можуть бути застосовані також параметризовані Т-норми та/або Т-конорми, в яких певний параметр може змінювати властивості оператора узагальнення.

Методи нечітких мір передбачають, що оцінки альтернатив у критеріях описуються функцією належності, заданої на множині критеріїв: $g_i(c_j): C \rightarrow [0, 1]$, а ваги критеріїв описуються нечіткою мірою, заданою також на множині критеріїв: $f(\cdot): 2^C \rightarrow [0, 1]$, де позначення 2^C використане для опису множини всіх підмножин множини C .

У випадку нечітких мір як оператор узагальнення використовується нечіткий інтеграл Сугено або Шоке. Відмінності між ними детально проаналізовані в роботі авторів [27]. Вони полягають у тому, що інтеграл Сугено використовує базис операторів логіки, а інтеграл Шоке – базис арифметичних операцій. Інтеграл Сугено має певну перевагу, яка полягає в тому, що він дає змогу визначити підмножину критеріїв, яка вплинула на результат інтегрування і таким чином пояснити одержану оцінку альтернативи. Крім того, інтеграл Сугено може моделювати поріг нечутливості, наявність якого природно притаманна складним системам.

Використання нечітко-інтегрального числення має кілька переваг.

По-перше, нечітка міра задана на множині всіх підмножин множини критеріїв, що забезпечує можливість моделювання залежностей і взаємодій між критеріями, а також синергетичних ефектів [28]. У цьому разі не потрібні спеціальні процедури для врахування міжкритеріальних кореляцій, які застосовуються в адитивних методах. Крім того, інші методи, які базуються на представленні множини визначення (базис міркувань) у вигляді традиційної множини з окремих елементів у принципі не можуть безпосередньо описати синергетичні ефекти, оскільки синергія породжується в результаті поєднання та взаємодії окремих елементів.

По-друге, нечітка міра має параметр нормування $\lambda \in [-1, \infty]$, який ще називають семантичним параметром. Він відображає семантику (значення, смисл) або модальність нечіткої міри, яка розглядається як відношення до дійсності змісту оцінок, описаних цією мірою. Для пояснення розглянемо приклад підкидання монети

і ставлення дослідника до результату. Якщо дослідник поставить собі запитання: «Яка можливість ($\lambda = 1$) випадання решки?», відповідь буде «одиниця», оскільки принципово ніщо не може завадити появі цього результату. Якщо поставити запитання: «Яка необхідність ($\lambda \rightarrow 0$) випадання решки?», відповіддю буде «нуль», оскільки жодних гарантій появи цього результату не існує. Як бачимо, сума оцінок двох несумісних подій може дорівнювати двом у випадку модальності «можливість» і нулю – у випадку модальності «необхідність». Між ними розташовані безліч відтінків модальності, в тому числі «ймовірність» ($\lambda = 0$), що підкреслює той факт, що нечітку міру можна розглядати параметричним розширенням міри ймовірності [26]. Таким чином, нечітка міра, на відміну від інших математичних конструкцій, додатково відображає відношення оцінок до дійсності, тобто забезпечує більшу адекватність оцінок тому смислу, який закладає людина у схему оцінювання.

По-третє, λ -параметр нечіткої міри налагоджує нечіткий інтеграл на певну логіку обчислення узагальненої оцінки. Наприклад, значення $\lambda = 1$ призводить до того, що результат нечіткого інтегрування стає аналогічним операції «АБО», а значення $\lambda \rightarrow \infty$ – операції «І». Тобто якщо міркувати в термінах логічних операцій, нечіткий інтеграл можна розглядати як універсальну процедуру нечіткої логіки для обчислення результату.

По-четверте, з погляду філософії розв'язання наукових задач методами штучного інтелекту застосування адитивних методів не є коректним, оскільки штучний інтелект моделює розумові процеси людини, але ці процеси не є адитивними.

Нейронні мережі є, мабуть, найпоширенішою технікою розв'язання задач оцінювання. На сьогодні відомо багато видів нейронних мереж, які є ефективними в різних особливих випадках, але класичною нейронною мережею залишається перцептрон Розенблатта, логічна схема якого показана на *рисунку 3*.

На вхід перцептрона надходить сигнал, який фіксується сенсорами. Вихідний сигнал сенсора може вимірюватись у шкалі $[0;1]$ або $[0,1]$. Ці сигнали передаються нейронам асоціативного шару. Кожний із цих нейронів має суматор і функцію порогу, яка моделює нечутливість до слабких сигналів (шумів) і призначена для придушення шумів. Далі сигнали, які пройшли поріг нечутливості, подаються на реагуючий нейрон та обробляються в аналогічному порядку.

Звернімо увагу, що ця схема дуже схожа з описаною вище концептуальною схемою на *рисунку 2*. Якщо в схемі на *рисунку 2* відобразити дискретні множини, на яких визначаються параметри альтернатив, то логічна схема перцептрона Розенблатта буде цілком еквівалентна концептуальній схемі розв'язання найпростішої задачі оцінювання. Крім того, якщо як передавальну функцію асоціативних і реагуючих нейронів використати нечіткий інтеграл, то й описаний вище порядок розв'язання задачі оцінювання буде еквівалентним порядку роботи нейрон-

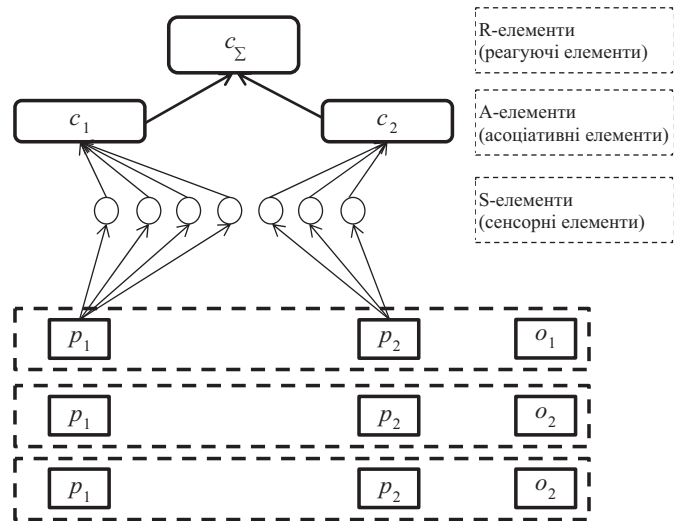


Рис. 3. Логічна схема перцептрона Розенблатта з одним виходом

ної мережі. Подібний приклад на основі використання нечіткого інтеграла Шоке описаний у роботі [29].

Таким чином, нейронні мережі можна вважати інструментами, певним чином еквівалентними методами техніки TOPSIS. Але щодо нейронних мереж особливий інтерес можуть мати алгоритми їхнього навчання, засновані на обробці досить великих масивів статистичних даних.

Розв'язання задач класифікації

Задача класифікації розглядається як оцінювання відповідності альтернативи опису певного класу. У такій постановці задача класифікації зводиться до кількох задач оцінювання, відповідно до кількості класів. Як і в задачі оцінювання, альтернативи описуються параметрами, а класи – еталонами, які можуть бути задані явно або неявно.

Головною особливістю класифікації є формулювання і властивості класів. Зокрема, класи можуть бути сформульовані як такі, що:

- цілком не схожі один з одним (чіткі класи);
- дещо схожі між собою (нечіткі класи);
- деякі класи є повністю вкладеними в інші класи (вкладені класи).

У разі використання одиничної шкали в першому випадку оцінки альтернативи дорівнюють або 1, або 0. При цьому оцінка 1 має зустрічатися лише один раз. Рішенням задачі буде той клас, де оцінка відповідності дорівнюватиме 1. У другому випадку оцінки набувають значень з діапазону $[0,1]$. Як рішення виступатиме той клас, у якому оцінка буде максимальною. При цьому максимальне значення оцінки також має зустрічатися лише один раз. У випадку вкладених класів оцінки альтернативи також набувають значень з діапазону $[0,1]$, але можуть бути максимальними в кількох класах.

Техніка розв'язання задачі класифікації для кожного класу цілком аналогічна концептуальній схемі розв'язання задач оцінювання, показаній на *рисунку 2*. Відмінність полягає лише в тому, що для кожного класу формується свій критерій верхнього рівня $c_{\Sigma}^{\text{class } \#...}$.

Аналогічно до того, що задача оцінювання може бути розв'язана на підставі різних методів (адитивних, таксономічних, нечітко-інтегрального числення тощо), задача класифікації також може бути розв'язана по-різному. Але існує одна ключова відмінність – задача класифікації вимагає того, щоб метод забезпечував достатню розрізненість (вибірковість) між класами, інакше класи будуть «зливатися». Як свідчить досвід розв'язання аналітичних задач на практиці, таку розрізненість краще забезпечують методи нечітких мір і нейронні мережі.

Розв'язання задач кластеризації

Задача кластеризації розглядається як задача розподілення множини альтернатив за класами еквівалентності. Задача виникає, коли кілька альтернатив потрібно згрупувати на основі значень їхніх параметрів. Розв'язання задачі передбачає виконання таких кроків: визначення відношення схожості і потім на його основі – відношення еквівалентності на множині альтернатив. Далі здійснюється формування кластерів.

У загальному випадку існують багато методів кластеризації, огляд яких наданий у дослідженні [30]. Найпоширенішим алгоритмом кластеризації є «C-Means», який передбачає поділ множини альтернатив на основі значень їхніх параметрів. Але в різних контекстах (ситуаціях) параметри альтернатив можуть розглядатися по-різному. Наприклад, в одному випадку виделка може розглядатися як елемент множини столового начиння, в іншому – множини знарядь убивства. Тому така кластеризація вимагає додавання в задачу категорії контексту.

Зазвичай це робиться шляхом відбору множини параметрів окремо в кожному конкретному випадку. Але це можна зробити, якщо значення параметрів альтернатив узагальнити за допомогою розв'язання задачі оцінювання [31]. Представлена на *рисунку 2* ієрархічна структура за сутністю описує неявний еталон, а оцінки є оцінками подібності цьому еталону. Еталон для альтернатив є контекстом їхньої оцінки. Змінюючи ваги критеріїв, ми змінюватиме контекст і можемо одержати безліч поділів. Методи штучного інтелекту тут застосовані для розв'язання задачі одержання оцінок подібності альтернатив.

Але останнім часом набули розвитку методи нечіткої кластеризації [32]. Вони спрямовані на розв'язання задач визначення так званих кластерних ансамблів – комбінацій чисельних поділів, одержаних на основі окремих розв'язків задач кластеризації, в кінцевий консенсусний поділ. Ці методи розглядаються як техніка одержання нових знань на підставі обробки великих масивів даних («BigData»). Показовим прикладом такої задачі є

визначення сегментації груп людей на підставі різних критеріїв: релігійних уподобань, потреб, демографії тощо.

Розв'язання задач вибору

У класифікації аналітичних задач [1] задача вибору належить до задач управління. Це багатоактні задачі (оптимального, сценарного чи ігрового управління), в яких вибір здійснюється в результаті виконання багатьох кроків, а також одноактні, зокрема задачі власне вибору і впорядкування. На найзагальнішому рівні концептуальну схему задачі управління можна подати як послідовність задачі оцінювання і задачі вибору з множини оцінених альтернатив з використанням додаткового критерію вибору.

Наприклад, досить поширеною є двокрокова техніка розв'язання багатокритеріальних задач вибору за допомогою методу Еджворта-Парето [33]. Спочатку одержують оцінки альтернатив в обраних критеріях вищого рівня узагальнення. Потім використовують певне правило регуляризації для одержання результуючих оцінок альтернатив. Як правило, цю техніку застосовують тоді, коли критерії важко порівняти між собою, щоб одержати відношення переваги. Але тут побудова відношення переваг на множині критеріїв де-факто замінена апріорним правилом регуляризації.

Однією з особливостей задач управління є унікальність структури, послідовності розв'язання і комбінування критеріїв, що продиктовано особливостями природи об'єкта управління і середовища його функціонування. Щоб продемонструвати таку особливість розглянемо приклад розв'язання задачі вибору найраціональнішого варіанта дій держави на воєнно-політичному рівні. Схожі задачі наявні серед багатьох задач стратегічного, оперативного і тактичного рівнів.

Нехай на поточний момент держава, виходячи з оцінки своїх ресурсів, спроможностей і політичної доцільності, сформувала множину варіантів дій $Z = \{z_1, z_2\}$. Здійснення зазначених дій у результаті може призвести до кількох ситуацій з множини $X = \{x_1, \dots, x_4\}$. Кожна із ситуацій може бути оцінена з погляду сприятливості, тобто відповідності національним інтересам, у певній впорядкованій множині оцінок $Y = \{y_1 = \text{«низька»}, y_2 = \text{«середня»}, y_3 = \text{«висока»}\}$.

Нехай у разі вибору варіанта дій z_1 є можливою поява ситуацій з підмножини $A \subseteq X = \{x_1, x_3\}$, а в разі вибору варіанта дій z_2 – ситуацій з підмножини $B \subseteq X = \{x_2, x_4\}$. Нехай також у результаті розв'язання задачі оцінювання визначені ступені сприятливості ситуацій, описані такою умовною нечіткою мірою:

$$\sigma_x(\cdot|y) = \begin{matrix} y_1 \\ y_2 \\ y_3 \end{matrix} \begin{bmatrix} 1 & 0.8 & 0.1 & 0.1 \\ 0.2 & 1 & 0.7 & 0.4 \\ 0.1 & 0.2 & 0.3 & 1 \end{bmatrix} \begin{matrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{matrix}.$$

Задача полягає у виборі варіанта дій, який би забезпечив сприятливість ситуації, не нижче за «середню».

Звернімо увагу на структуру задачі. Напрошується запитання: чи можна спростити задачу й оцінювати одразу варіанти дій на відповідність національним інтересам. Відповідь: ні, не можна, оскільки послідовність «дія – ситуація – оцінка ступеня сприятливості» існує саме в такому вигляді та її спрощення призведе до викривлення природи задачі. Це є головною особливістю природи цієї задачі.

Розв'язання задачі передбачає розв'язання двох підзадач:

Підзадача 1. Одержати розподіл упевненості у сприятливості ситуації в разі реалізації варіанта дій.

Скористаймося властивістю умовних нечітких мір. Зокрема, для будь-якої підмножини $E \subseteq X$ умовна нечітка міра $\sigma_x(\cdot | y)$ є функцією належності на просторі Y : $\sigma_x(E | y): Y \rightarrow [0,1]$. З іншого боку, для будь-якого елемента $y \in Y$ умовна нечітка міра $\sigma_x(\cdot | y)$ є нечіткою мірою на просторі X : $\sigma_x(E | y): 2^X \rightarrow [0,1]$.

Розгляньмо нечіткі міри $\forall y_i, i = \overline{1,3}$, $\sigma_x(\cdot | y): 2^X \rightarrow [0,1]$. Оскільки виконується умова $\forall y_i, i = \overline{1,3}, \sup_{x \in X} \sigma_x(x | y_i) = 1$, то для кожного

$\forall y_i, i = \overline{1,3}$ нечітка міра є мірою можливості. Отже, виконується умова:

$$\forall i \in I, A \subseteq X, Poss(\bigcup_{i \in I} A_i) = \sup_{i \in I} \{Poss(A_i)\}.$$

Тоді для варіанта $z_1, A \subseteq X = \{x_1, x_3\}$ маємо:

$$\begin{aligned} y_1 \in Y &\Rightarrow \sigma_X(\{x_1, x_3\} | y_1) = \\ &= \sigma_X(\{x_1\} | y_1) \vee \sigma_X(\{x_3\} | y_1) = 1 \vee 0.1 = 1; \\ y_2 \in Y &\Rightarrow \sigma_X(\{x_1, x_3\} | y_2) = 0.2 \vee 0.7 = 0.7; \\ y_3 \in Y &\Rightarrow \sigma_X(\{x_1, x_3\} | y_3) = 0.1 \vee 0.3 = 0.3. \end{aligned}$$

Аналогічно для варіанта $z_2, B \subseteq X = \{x_2, x_4\}$ маємо:

$$\begin{aligned} y_1 \in Y &\Rightarrow \sigma_X(\{x_2, x_4\} | y_1) = 0.8 \vee 0.1 = 0.8; \\ y_2 \in Y &\Rightarrow \sigma_X(\{x_2, x_4\} | y_2) = 1 \vee 0.4 = 1; \\ y_3 \in Y &\Rightarrow \sigma_X(\{x_2, x_4\} | y_3) = 0.2 \vee 1 = 1. \end{aligned}$$

Підзадача 2. Здійснити вибір варіанта дій, виходячи із забезпечення заданого рівня сприятливості ситуації.

Для дій z_1, z_2 оцінки сприятливості ситуації не нижче «середня» визначатимуться співвідношеннями відповідно:

$$\begin{aligned} y_2 y_3 \in Y &\Rightarrow \sigma_X(\{x_1, x_3\} | y_2) \vee \sigma_X(\{x_1, x_3\} | y_3) = \\ &= 0.7 \vee 0.3 = 0.7 \end{aligned}$$

та

$$y_2 y_3 \in Y \Rightarrow \sigma_X(\{x_2, x_4\} | y_2) = \sigma_X(\{x_2, x_4\} | y_3) = 1 \vee 1 = 1.$$

Отже, найсприятливішу ситуацію з погляду національних інтересів забезпечуватиме дія держави z_2 .

Розв'язання задач прогнозування

У загальному випадку прогноз – це обґрунтоване судження про можливий стан (стани) об'єкта в майбутньому, а також про шляхи й терміни його досягнення. Оскільки стан об'єкта, як правило, описується оцінками, то в технологічному сенсі сутність задачі прогнозування полягає в одержанні оцінки альтернативи в майбутньому. При цьому головним питанням є питання парадигми, обраної для опису часу. Це питання й сьогодні залишається найсуперечливішим. Але все ж можна виокремити три загальні техніки прогнозування:

- статистичну: вивчення статистичних трендів оцінок у минулому, виявлення їхнього характеру і продовження трендів у майбутньому на підставі припущення про стабільність характерних рис;
- сценарну: вивчення умов існування досліджуваного об'єкта, висунення на цій підставі припущень щодо змін умов у майбутньому та щодо їхніх можливих сполучень (сценаріїв), як правило позитивного, негативного і нейтрального з погляду дослідника;
- подієву: висунення припущень щодо подій, які можуть відбутись у майбутньому (виходячи з логіки розвитку системи, де існує досліджуваний об'єкт), і припущень щодо впливу цих подій.

Статистична техніка передбачає спочатку побудову явного чи неявного полінома на основі статистичних оцінок та його подальше «продовження» в часі на основі екстраполяції. Тут одна з основних можливостей застосування методів штучного інтелекту полягає в представленні змінних і коефіцієнтів поліномів у вигляді нечітких чисел $\bar{N}: \mathbb{R} \rightarrow [0,1]$ (див., наприклад, [34]) та обрахунку полінома за допомогою нечітких арифметичних операцій.

Сценарна техніка передбачає насамперед вибір парадигми для опису умов існування досліджуваного об'єкта і методу генерування сценаріїв. Для опису умов можуть використовуватися ймовірнісні розподіли, нечіткі функції належності або нечіткі міри. Генерування сценаріїв передбачає визначення сполучень значень параметрів згаданих вище умов. Огляд методів генерування сценаріїв для випадку ймовірнісних розподілів наведений у [35]. Наприклад, дослідження [36] описує метод генерації сценаріїв для випадку нечітких функцій належності.

Подієва техніка є ефективною у випадках значної невизначеності, коли аналітичну задачу неможливо розв'язати без участі людини, а також за відсутності або невалідності статистики. Технологічно вона зводиться до розв'язання кількох задач оцінювання відповідно до кількості моментів часу, що обраховуються. При цьому

в кожний момент часу на параметри задачі діє певна множина подій, яка змінює ці параметри і за рахунок цього зсуває узагальнену оцінку, одержуючи таким чином прогноз. Техніка передбачає припущення щодо появи в майбутньому певних подій, результатом чого є «зсув» або значень параметрів альтернатив, або важливості критеріїв. Тут головними питаннями є генерація подій і розрахунок ступеня й напряду сукупного впливу кількох подій на параметри альтернатив або ваги критеріїв. Підходи до розв'язання цих питань наведені в дослідженнях [19] та [37] відповідно.

Розв'язання задач чисельних розрахунків

Чисельні розрахунки зустрічаються майже в усіх прикладних задачах, пов'язаних з тактичними, оперативними, логістичними тощо розрахунками. Загальної концептуальної схеми розв'язання цієї задачі не існує, оскільки в кожному конкретному випадку вона визначається логікою розрахунків. По суті, це послідовність арифметичних операцій.

На практиці всі такі операції пов'язані із числовою невизначеністю. Наприклад, ми не можемо точно знати кількість особового складу штурмових підрозділів противника або кількість його танків, бронемашин тощо. Під час планування розподілу та підвезення боєприпасів їхня точна кількість у підрозділах невідома, оскільки тривають бойові дії та відбуваються постійні витрати мінливої інтенсивності. Відомі задачі, де подібна невизначеність описується за допомогою ймовірності. Але ж, як було показано вище, ймовірнісні методи є адитивними. Вони мають негативну властивість компенсації одних значень іншими, а також вимагають незалежності величин, які взаємодіють в арифметичних операціях, що не завжди можливо забезпечити.

Виходом може бути використання нечітких чисел, точніше, нечітких числових множин, які були запропоновані Л. Заде [38]. У загальному випадку нечітким числом A називається нечітка множина з носієм, визначеним на множині дійсних чисел:

$$A = \{(x, y) \in \mathbb{R} \times [0, 1] : y = \mu_A(x)\},$$

де $\mu_A(x)$ – функція належності A . Будь-яка операція $\otimes$ із чотирьох арифметичних операцій між нечіткими числами A та B визначається відповідно до принципу розширення Заде:

$$\mu_C(z) = \sup_{z=x \otimes y} \min \{\mu_A(x), \mu_B(y)\}, x, y, z \in \mathbb{R},$$

де $\mu_C(z)$ – функція належності результуючого числа $C = A \otimes B$.

Але відчутними проблемами цього класичного підходу є складність забезпечення відповідності властивостей нечітких операцій властивостям операцій традиційної арифметики, а також ефект «розповзання носія» в результаті виконання послідовності розрахунків, унаслідок чого невизначеність розв'язку необмежено зростає.

Для розв'язання першої проблеми були запропоновані кілька модифікацій класичних нечітких чисел, наприклад нечіткі числа Атанасова [39]. Для розв'язання другої проблеми авторами був запропонований алгоритм [40], заснований на пошуку нечіткого числа з максимальною ентропією. Цей алгоритм автори реалізували як надбудову для Microsoft Excel, яку можна безкоштовно скачати за посиланням:

<https://www.dropbox.com/s/2qre4sfuo3jawie/Fuzzy%20for%20Excel%2064bit.zip?dl=0>

Висновок

На жаль, обмеження обсягу статті не дають змоги викласти всі нюанси використання сучасних методів штучного інтелекту для розв'язання наукових задач у сфері оборони. Але автори мають надію, що викладені матеріали будуть достатніми, щоб хоча б у першому наближенні продемонструвати можливості цих методів, їхню простоту й ті втрати, які ми робимо, приділяючи їм недостатньо уваги.

Перелік літератури

1. Технологія аналізу воєнно-політичної обстановки / В. П. Бочарніков, С. В. Свешніков, Р. І. Тимошенко, В. І. Павленко. – К. : НУОУ ім. Івана Черняхівського, 2019. – 384 с.
2. Російсько-українська війна: особливості реалізації загроз державному суверенітету України та перспективи виходу з війни [Електронний ресурс] / М. М. Шевченко, О. С. Зозуля, Г. С. Храпач, А. В. Лепіхов // Збірник наукових праць ЦВСД НУОУ ім. І. Черняхівського. – 2022. – № 2 (75). – С. 6–15. – Режим доступу : <https://doi.org/10.33099/2304-2745/2022-2-75/6-15>.
3. Іващенко А. М. Прогнозування розвитку конфліктів гібридного типу на основі Big Data [Електронний ресурс] / А. М. Іващенко // Збірник наукових праць ЦВСД НУОУ ім. І. Черняхівського. – 2021. – № 3 (73). – С. 42–47. – Режим доступу : <https://doi.org/10.33099/2304-2745/2021-3-73/42-47>.
4. Вітер Д. В. Застосування сил спеціальних операцій у багатосферних операціях [Електронний ресурс] / Д. В. Вітер // Збірник наукових праць ЦВСД НУОУ ім. І. Черняхівського. – 2022. – № 3 (76). – С. 6–12. – Режим доступу : <https://doi.org/10.33099/2304-2745/2022-3-76/6-12>.
5. Searle T. Outside the Box: A New General Theory of Special Operations : JSOU Report 17-4 / T. Searle ; Joint Special Operations University. – MacDill Air Force Base : JSOU Press, 2017. – XII, 66 p.
6. Іващенко А. М. Концепція багатодомених операцій та її застосування силами оборони [Електронний ресурс] / А. М. Іващенко, В. В. Гордійчук, Н. М. Андріянова // Збірник наукових праць ЦВСД НУОУ ім. І. Черняхівського. – 2022. – № 3 (76). – С. 62–67. – Режим доступу : <https://doi.org/10.33099/2304-2745/2022-3-76/62-67>.
7. Момот Д. С. Рекомендації щодо визначення кількості та складу мобільних протидиверсійних резервів під час оперативного розгортання військ оперативного командування в інтересах оборонної операції об'єднаних сил [Електронний ресурс] / Д. С. Момот // Збірник наукових праць ЦВСД НУОУ ім. І. Черняхівського. – 2022. – № 3 (76). – С. 86–91. – Режим доступу : <https://doi.org/10.33099/2304-2745/2022-3-76/86-91>.

8. Хімченко О. С. Формалізація завдання з дезорганізації системи управління військами (силами) противника під час нанесення зустрічного удару ракетними військами [Електронний ресурс] / О. С. Хімченко // Збірник наукових праць ЦВСД НУОУ ім. І. Черняхівського. – 2022. – № 2 (75). – С. 26–32. – Режим доступу : <https://doi.org/10.33099/2304-2745/2022-2-75/26-32>.
9. Слісар П. О. Удосконалена методика визначення ймовірності досягнення потрібного ефекту координації вогневого ураження противника в операції [Електронний ресурс] / П. О. Слісар // Збірник наукових праць ЦВСД НУОУ ім. І. Черняхівського. – 2022. – № 2 (75). – С. 40–46. – Режим доступу : <https://doi.org/10.33099/2304-2745/2022-2-75/40-46>.
10. Кацалан В. О. Методичний підхід до оцінювання рівня інформаційно-психологічного впливу противника в інтересах інформаційної операції Збройних Сил України [Електронний ресурс] / В. О. Кацалан, О. Д. Кирпичников, Р. Д. Саунін // Збірник наукових праць ЦВСД НУОУ ім. І. Черняхівського. – 2022. – № 3 (76). – С. 24–31. – Режим доступу : <https://doi.org/10.33099/2304-2745/2022-3-76/24-31>.
11. Методичний підхід до управління ризиками безпеки інформації як складової забезпечення інформаційної безпеки держави [Електронний ресурс] / П. М. Сніцаренко, Ю. А. Саричев, В. П. Зубков, Ю. А. Піщанський // Збірник наукових праць ЦВСД НУОУ ім. І. Черняхівського. – 2022. – № 2 (75). – С. 47–55. – Режим доступу : <https://doi.org/10.33099/2304-2745/2022-2-75/47-55>.
12. Підходи до оцінювання захищеності інформаційної інфраструктури Міністерства оборони України [Електронний ресурс] / А. А. Рибидайло, В. А. Федорієнко, О. С. Кульчицький, Є. Г. Обозненко // Збірник наукових праць ЦВСД НУОУ ім. І. Черняхівського. – 2022. – № 1 (74). – С. 69–77. – Режим доступу : <https://doi.org/10.33099/2304-2745/2022-1-74/69-77>.
13. Застосування дата-центричного підходу під час побудови інформаційної інфраструктури з використанням хмарних технологій для оборонних потреб [Електронний ресурс] / Ю. А. Кирпичников, В. О. Капілевич, О. В. Андрощук, М. В. Петрушен // Збірник наукових праць ЦВСД НУОУ ім. І. Черняхівського. – 2022. – № 3 (76). – С. 68–75. – Режим доступу : <https://doi.org/10.33099/2304-2745/2022-3-76/68-75>.
14. Аналіз підходів до оцінювання психофізіологічного стану воїнів Сил оборони України за допомогою мініатюрних кардіографічних засобів [Електронний ресурс] / М. М. Бочаров, В. Г. Дикун, І. А. Чайковський та ін. // Збірник наукових праць ЦВСД НУОУ ім. І. Черняхівського. – 2022. – № 3 (76). – С. 76–85. – Режим доступу : <https://doi.org/10.33099/2304-2745/2022-3-76/76-85>.
15. Аналіз стану заходів протидії корупції в Міністерстві оборони України та Збройних Силах України за 2018–2020 роки [Електронний ресурс] / П. В. Жук, В. В. Бевз, С. С. Гайдаров та ін. // Збірник наукових праць ЦВСД НУОУ ім. І. Черняхівського. – 2022. – № 3 (76). – С. 92–100. – Режим доступу : <https://doi.org/10.33099/2304-2745/2022-3-76/92-100>.
16. Загорка О. М. Розвиток зенітних ракетних комплексів і систем для оборони військ та об'єктів від ударів нестратегічних балістичних ракет [Електронний ресурс] / О. М. Загорка, О. В. Дейнега // Збірник наукових праць ЦВСД НУОУ ім. І. Черняхівського. – 2022. – № 2 (75). – С. 16–25. – Режим доступу : <https://doi.org/10.33099/2304-2745/2022-2-75/16-25>.
17. Saaty T. L. Analytical planning: the organization of systems / T. L. Saaty, K. P. Kearns. – Oxford : Pergamon Press, 1985. – VII, 208 p. – (International series in modern applied mathematics and computer science ; vol. 7).
18. Li J. J. An MCDM model based on KL-AHP and TOPSIS and its application to weapon system evaluation [Електронний ресурс] / J. J. Li, L. W. Liu // Proceedings of the 5th International Asia Conference on Industrial Engineering and Management Innovation (IEMI2014). – Режим доступу : https://link.springer.com/chapter/10.2991/978-94-6239-100-0_48.
19. Bocharnikov V. Metric on the space of systems behavior functions represented by fuzzy measures [Електронний ресурс] / V. Bocharnikov, S. Sveshnikov // Yugoslav Journal of Operations Research. – 2023. – OnLine-First Issue. – Режим доступу : <https://doi.org/10.2298/YJOR230315012B>.
20. Gao F. Weapon system operational effectiveness evaluation based on the belief rule-based system with interval data [Електронний ресурс] / F. Gao, A. Zhang, W. Bi // Journal of Intelligent & Fuzzy Systems. – 2020. – Vol. 39, issue 5. – P. 6687–6701. – Режим доступу : <https://doi.org/10.3233/JIFS-190651>.
21. Свешніков С. В. Ентропійний алгоритм нечіткої арифметики / С. В. Свешніков // Наук.-техн. зб. ННДЦ ОТ і ВБ України. – 2002. – Вип. 13. – С. 14–25.
22. Zhang S. T. Evaluation of Capability of Weapon System of Systems Based on Multi-Scenario [Електронний ресурс] / S. T. Zhang, Y. J. Dou, Q. S. Zhao // Advanced Materials Research. – 2014. – Vols. 926–930. – P. 3806–3811. – Режим доступу : <https://doi.org/10.4028/www.scientific.net/AMR.926-930.3806>.
23. Measuring national power in the postindustrial age [Електронний ресурс] / A. J. Tellis, J. Bially, C. Layne, M. McPherson. – Santa Monica : RAND, 2000. – XVI, 198 p. – Режим доступу : <https://apps.dtic.mil/sti/pdfs/ADA386226.pdf>.
24. Косецов В. О. Національна безпека України: теорія, реальність, прогноз : монографія / В. О. Косецов ; Центр міжнародної безпеки та стратегічних студій. – К. : Сатсанга, 2000. – 80 с.
25. Deza M. Encyclopedia of distances / M. Deza, E. Deza. – 4th ed. – Berlin : Springer, 2016. – XXII, 756 p.
26. Нечеткие множества в моделях управления и искусственного интеллекта / А. Н. Аверкин, И. З. Батыршин, А. Ф. Блишун и др. ; под ред. Д. А. Поспелова. – М. : Наука, 1986. – 312 с. – (Проблемы искусственного интеллекта ; т. 8).
27. Estimating the potential willingness of the state to use military force based on the Sugeno fuzzy integral [Електронний ресурс] / S. Sveshnikov, V. Bocharnikov, A. Pavlikovsky, A. Prima // Yugoslav Journal of Operations Research. – 2022. – Vol. 32, No 3. – P. 325–356. – Режим доступу : <http://dx.doi.org/10.2298/YJOR210515002S>.
28. Свешніков С. В. Врахування синергетичних втрат ефективності бойової системи на основі нечіткої міри Сугено / С. В. Свешніков, В. П. Бочарников, О. С. Хімченко // Труды университета. – 2022. – № 2 (171). – С. 35–51.
29. Chiang J. H. Choquet fuzzy integral-based hierarchical networks for decision analysis [Електронний ресурс] / J. H. Chiang // IEEE Transactions on Fuzzy Systems. – 1999. – Vol. 7, issue 1. – P. 63–71. – Режим доступу : <https://doi.org/10.1109/91.746311>.
30. Madhulatha T. S. An overview on clustering methods [Електронний ресурс] / T. S. Madhulatha // IOSR Journal of Engineering. – 2012. – Vol. 2, issue 4. – P. 719–725. – Режим доступу : <https://doi.org/10.9790/3021-0204719725>.

31. Бочарніков В. П. Алгоритм кластеризації військово-політичних сил в умовах невизначеності / В. П. Бочарніков, С. М. Возняк // Наук-техн. зб. ННДЦ ОТ і ВБ України. – 1999. – Вип. 3. – С. 35–41.
32. Advances in fuzzy clustering and its applications / edited by J. V. de Oliveira, W. Pedrycz. – Chichester : John Wiley & Sons, 2007. – XX, 434 p.
33. Ногин В. Д. Обобщенный принцип Эджворта-Парето в терминах функций выбора / В. Д. Ногин // Труды ИСА РАН. – 2005. – Т. 12. – С. 43–53.
34. Mosleh M. Fuzzy polynomial regression with fuzzy neural networks [Електронний ресурс] / М. Mosleh, М. Otadi, S. Abbasbandy // Applied mathematical modelling. – 2011. – Vol. 35, issue 11. – P. 5400–5412. – Режим доступу : <https://doi.org/10.1016/j.apm.2011.04.039>.
35. Kaut M. Evaluation of scenario-generation methods for stochastic programming [Електронний ресурс] / М. Kaut, W. Stein // Stochastic Programming E-print Series (SPEPS). – Vol. 2003. – Режим доступу : <https://doi.org/10.18452/8296>.
36. A fuzzy inference based scenario building in two-stage optimization framework for sustainable recycling supply chain redesign [Електронний ресурс] / М. Feitó-Cespón, Y. Costa, M. S. Pishvae, R. Cespón-Castro // Expert Systems with Applications. – 2021. – Vol. 165. – Art. 113906. – Режим доступу : <https://doi.org/10.1016/j.eswa.2020.113906>.
37. Sveshnikov S. Forecasting financial indexes with model of composite events influence / S. Sveshnikov, V. Bocharnikov // Journal of Applied Economic Sciences. – 2009. – Vol. 4, issue 9. – P. 425–440.
38. Zadeh L. A. The Concept of linguistic variable and its application to approximate reasoning [Електронний ресурс] / L. A. Zadeh // Information Sciences. – 1975. – Vol. 8, issue 4. – P. 301–357. – Режим доступу : [https://doi.org/10.1016/0020-0255\(75\)90046-8](https://doi.org/10.1016/0020-0255(75)90046-8).
39. Nehi H. M. Intuitionistic fuzzy numbers and its applications in fuzzy optimization problem / H. M. Nehi, H. R. Maleki // Proceedings of the 9th WSEAS International Conference on Systems, 11–13 July 2005, Athens, Greece / edited by I. W. Sandberg. – Stevens Point : WSEAS, 2005. – P. 1–5.
40. Sveshnikov S. Computational Algorithm and Tools of Fuzzy Arithmetic Based on the Principle of Maximum Entropy [Електронний ресурс] : preprint / S. Sveshnikov, V. Bocharnikov // Research Square. – Режим доступу : <https://doi.org/10.21203/rs.3.rs-1254409/v1>.

DOI 10.33099/2618-1614-2023-23-4-41-47

УДК 623.442.4

В. М. Сенаторов,*кандидат технічних наук, доцент, старший науковий співробітник, Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України,***А. В. Гурнович,***доктор технічних наук, професор, провідний науковий співробітник, Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України,***Б. О. Мельник,***кандидат технічних наук, старший науковий співробітник, начальник науково-дослідного відділу, Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, полковник,***А. В. Кучинський,***кандидат технічних наук, старший науковий співробітник, докторант, Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України, полковник*

Застосування стрілецької зброї для знищення дрона-камікадзе «Шахед-136»

В інформаційному полі надаються рекомендації щодо поправок на випередження при стрільбі по дрону-камікадзе «Шахед-136», які суттєво різняться за даними. Ці суперечливі дані визначили мету статті – розробку методики розрахунку випередження і верифікацію рекомендацій щодо обстрілу дронів-камікадзе типу «Шахед-136» стрілецькою зброєю. У статті на базі розробленої теорії окомірного способу прицілювання проведена верифікація відомих рекомендацій. Надані рекомендації щодо поправок на випередження при використанні стрілецької зброї, яка перебуває на озброєнні Збройних Сил України, з урахуванням балістичної функції. Сформовані пропозиції щодо вдосконалення кулеметної установки, яка успішно використовується військовослужбовцями Національної гвардії України, і створення для неї перспективної прицільної системи.

Ключові слова: Шахед-136, стрілецька зброя, випередження, прицільний пристрій.

© В. М. Сенаторов, А. В. Гурнович, Б. О. Мельник, А. В. Кучинський, 2023

Постановка задачі. Нині існує декілька способів та апаратури для знищення безпілотних літальних апаратів (БпЛА): системи проти-повітряної оборони, придушення сигналу за допомогою систем радіоелектронної боротьби, ловля сітками, зіткнення з апаратами-перехоплювачами, стрілецька зброя [1]. Методи відрізняються дистанцією ураження та кінцевим результатом: БпЛА може бути повністю знищений або захоплений практично не ушкодженим

На нашу думку, найефективнішим способом знищення БпЛА-камікадзе є супроводжувальна стрільба. При цьому потрібно враховувати поправки на випередження при обстрілі баражуючого боеприпасу.

В інформаційному полі надаються рекомендації щодо поправок на випередження, які суттєво різняться за даними. Наприклад, у джерелах [2, 3] наведено дані щодо вибору точки прицілювання для знищення дрона-камікадзе «Шахед-136». У таблицях 1 і 2 надані рекомендовані значення випередження для двох значень дистанції до цілі, трьох значень калібру і різного напрямку руху при швидкості цілі $V_u = 45$ м/с без зазначення типу зброї та швидкості кулі. Судячи з того, що в таблицях 1 і 2 вказані однакові значення швидкості, мова йде про дульну швидкість кулі. При цьому балістична функція не враховується. Аналіз стрілецької зброї, яка перебуває на озброєнні Збройних Сил України і може використовуватися для знищення дрона-камікадзе, показує, що тільки швидкість кулі 900 м/с відповідає дульній швидкості АК74. Решта значень швидкості є гіпотетичною: дульна швидкість зброї калібру 7,62 мм (АКМ, РПК, ПКМ, ПКТ) становить відповідно 715, 745, 825 і 855 м/с; дульна швидкість зброї калібру 12,7 мм (ДШКМ, НСВ) складає 820 м/с.

В іншому джерелі [4] рекомендовано для ураження дрона «Герань-2» (російський варіант дрона-камікадзе «Шахед-136») брати випередження із запасом (загороджувальна стрільба) і вести вогонь 1...2 с у фіксовану точку на шляху дрона, не рухаючи зброю. У таблиці 3 наведені рекомендовані значення випередження для різної дистанції D до цілі без зазначення її висоти H і характеру руху і типу зброї та її калібру.

Для знищення дрона рекомендується використовувати «різні модифікації кулемета Калашникова (ПКМ), установленого на зенітний станок у кузові пікапа, ручний кулемет Калашникова і модернізований автомат Калашникова з відповідним боеприпасом» [4]. Це збігається з результатами використання кулеметної установки на пікапі, розробленої фахівцями Національної гвардії України [5] з двома кулеметами ПКТ і зенітним прицільним пристроєм. У [4] також не рекомендовано використовувати снайперську гвинтівку і важкий крупнокаліберний кулемет, оскільки для ураження дрона на середній висоті польоту (до 800 м) потужність великого калібру буде надлишковою. Останнє не збігається з оцінкою ефективності вогню залежно від калібру зброї [3].

$$\text{ЦЦ}_y = D \sin(\psi) / \sin(\psi + q) \quad (6)$$

або значення випередження, виражене в кількості фігур БпЛА:

$$\text{ЦЦ}_y = D \sin(\psi) / B \sin(\psi + q), \quad (7)$$

де B – довжина фюзеляжу БпЛА, а кути q та ψ розраховуються відповідно за формулами (3) і (4) або (5).

Вирази (6) і (7) використаємо для верифікації даних, наведених у *таблицях 1, 2 і 3*. Як вихідні дані приймемо швидкість цілі $V_{\text{ц}} = 45$ м/с; довжину фюзеляжу $B = 3$ м; $\sin(q') = 3/4$ при скісному русі цілі: $q' = 48,6^\circ$.

При фронтальному і фланговому русі цілі формула (3) суттєво спрощується: $\sin(q) = H/D$ при фронтальному русі та $\sin(q) = 1$ при фланговому русі.

Верифікація даних таблиць

У *таблицях 5 і 6* наведені результати верифікації даних *таблиць 1 і 2* за формулами (3), (4), (6) і (7). Для визначення середньої швидкості кулі $V_{\text{к.сер}}$ використано балістичний калькулятор. Дані розрахунків $V_{\text{к.сер}}$ наведені в *таблиці 4*.

Таблиця 4

Значення середньої швидкості кулі

Зброя	Дистанція до цілі 360 м		Дистанція до цілі 728 м	
	Час польоту кулі, с	Середня швидкість кулі, м/с	Час польоту кулі, с	Середня швидкість кулі, м/с
АК74	0,453	795	1,341	543
АКМ	0,594	606	1,759	414
НСВ	0,425	847	1,047	695

Таблиця 5

Значення випередження (кількість фігур БпЛА довжиною 3 м) на дистанції до цілі 360 м (висота 200 м, дальність до проєкції цілі на землю 300 м)

Калібр / дульна швидкість кулі $V_{\text{к.0}}$, м/с	Характер руху цілі:		
	фланговий	фронтальний (на стрільця)	скісний, $q' = 48,6^\circ$
5,45/900 (АК)	7 (+1)	6 (+1)	7 (+1)
7,62/715 (АКМ)	9 (+2)	8 (+2)	9 (+2)
12,7/820 (НСВ)	6 (–1)	6 (0)	6 (–1)

Примітка: у *таблицях 5 і 6* у дужках наведена різниця між значеннями, розрахованими авторами, і значеннями, наведеними в *таблицях 1 і 2*.

Таблиця 6

Значення випередження (кількість фігур БпЛА довжиною 3 м) на дистанції до цілі 728 м (висота 200 м, дальність до проєкції цілі на землю 700 м)

Калібр / дульна швидкість кулі $V_{\text{к.0}}$, м/с	Характер руху цілі:		
	фланговий	фронтальний (на стрільця)	скісний, $q' = 48,6^\circ$
5,45/900 (АК)	20(+8)	11(0)	19(+7)
7,62/715 (АКМ)	32(+17)	15(+1)	24(+9)
12,7/820 (НСВ)	16(+2)	9(–4)	15(+1)

З даних *таблиці 3* випливає, що в розрахунках прийнята середня швидкість кулі кулемета ПКМ залежно від дальності до цілі. Відсутність даних щодо висоти і прийнятої швидкості цілі не дають змоги використати формули (3), (4), (6) і (7). Тому для верифікації даних *таблиці 3* використовується спрощена методика. Згідно із [7] лінійне випередження ЦЦ_y розраховується за формулами:

$$\text{ЦЦ}_y \approx D V_{\text{ц}} / V_{\text{к.сер}} \quad (8)$$

або значення випередження, виражене в кількості фігур БпЛА:

$$\text{ЦЦ}_y \approx D V_{\text{ц}} / B V_{\text{к.сер}}. \quad (9)$$

У *таблиці 7* наведені результати верифікації даних *таблиці 3* за формулами (8) і (9) при $V_{\text{ц}} = 45$ м/с, $B = 3$ м, $H = 200$ м і $V_{\text{к.сер}}$ 633, 675, 534 м/с відповідно для дистанції до цілі 200, 500, 800 м.

Таблиця 7

Значення випередження

Дистанція до цілі, м	200	500	800
Розрахункове значення випередження, м / кількість фігур БпЛА	14,2/ 5(0)	33,3/ 11(–2)	67,4/ 22(–2)

Примітка: у *таблиці 7* у дужках наведена різниця між значеннями, розрахованими авторами, і значеннями, наведеними в *таблиці 3*, виражена в кількості фігур БпЛА.

Що стосується поправки на зниження кулі, то траєкторія куль може не бути в наявності у стрільця. Тому необхідно оцінити зниження кулі η , виходячи з теорії руху тіла, кинутого під кутом до горизонту [6]:

$$\eta = 4,9(D_y / V_{\text{к.0}})^2 g_{\eta}, \quad (10)$$

де g_{η} – балістична функція.

Максимальне значення η має місце при максимумі відношення $D_y/V_{\text{к.0}}$. При фланговому русі D_y визначається за формулою:

$$D_y = [D^2 + (\text{ЦЦ}_y)^2]^{0,5},$$

і максимальне значення η визначається за формулою (10). Зокрема, при $D = 728$ м, $V_{к.сер} = 543$ м/с та $ЦЦ_y = 60,3$ м (дані таблиць 4 та 6): $\eta = 9$ м.

При фронтальному русі D_y визначається за формулою:

$$D_y = \{H^2 + [(D^2 - H^2)^{0,5} - ЦЦ_y]^2\}^{0,5},$$

і максимальне значення η знаходиться за формулою (10). Зокрема, при $D = 728$ м, $V_{к.сер} = 543$ м/с та $ЦЦ_y = 33,6$ м (дані таблиць 4 та 6): $\eta = 8$ м.

Як бачимо, зниження кулі перевищує габаритні розміри дрона-камікадзе «Шахед-136», тому необхідно вводити поправку на зниження кулі або застосовувати траєкторію кулі.

Аналіз таблиць 5–7 показує, що значення випередження, рекомендовані в джерелах [2–4], не суттєво відрізняються від даних верифікації на малій дистанції до цілі і суттєво відрізняються на великій. Це можна пояснити неврахуванням балістичного коефіцієнта.

Зрозуміло, що для знищення дрона-камікадзе можуть застосовуватися всі типи стрілецької зброї, які перебувають на озброєнні ЗСУ. У таблицях 8, 9 і 10 наведені розраховані значення випередження для цієї зброї для дистанції до цілі в діапазоні 300–800 м при висоті польоту 200 м, різного напрямку руху, швидкості цілі 45 м/с, з використанням балістичного калькулятора і робочих формул (3)–(7).

Вочевидь, що навіднику-оператору в напруженій бойовій обстановці важко на око чітко визначити кількість фігур БпЛА, тому можливі промахи під час стрільби. Тому на перший план виходить завдання автоматизації процесу прицілювання. Проблему, що виникатиме при конвертації балістичних коефіцієнтів куль, визначених за законом опору повітря 1943 року (притаманна для розрахунків у СРСР та Росії), до вигляду законів G1 та G7, що використовуються для

Таблиця 8

Значення випередження
(кількість фігур БпЛА довжиною 3 м)
у разі флангового руху цілі

Зброя	Дистанція до цілі, м					
	300	400	500	600	700	800
АК74	5	8	11	15	19	24
РПК74	5	7	10	14	17	24
АКМ	7	10	15	20	25	31
РПК	7	10	14	19	24	30
ПКМ (ПК)	6	8	11	15	18	23
ПКТ	5	8	11	14	18	22
ДШКМ (ДШК)	5	7	10	12	15	17
НСВ (НСВТ)	5	7	10	12	15	18
КПВТ	5	7	9	12	13	15

Таблиця 9

Значення випередження
(кількість фігур БпЛА довжиною 3 м)
у разі фронтального руху цілі

Зброя	Дистанція до цілі, м					
	300	400	500	600	700	800
АК74	5	8	11	14	18	22
РПК74	5	7	10	13	16	20
АКМ	7	10	14	18	23	28
РПК	6	10	13	18	22	27
ПКМ (ПК)	5	8	11	14	17	21
ПКТ	5	8	10	13	17	20
ДШКМ (ДШК)	5	7	9	12	14	16
НСВ (НСВТ)	5	7	10	12	15	17
КПВТ	5	6	8	10	13	15

Таблиця 10

Значення випередження
(кількість фігур БпЛА довжиною 3 м)
у разі скісного руху цілі ($q' = 48,6^\circ$)

Зброя	Дистанція до цілі, м					
	300	400	500	600	700	800
АК74	5	8	11	14	18	23
РПК74	5	8	10	13	17	23
АКМ	7	10	14	19	24	29
РПК	7	10	12	18	23	28
ПКМ (ПК)	6	8	11	14	18	22
ПКТ	5	8	11	14	17	21
ДШКМ (ДШК)	5	7	10	12	14	17
НСВ (НСВТ)	5	7	10	12	15	17
КПВТ	5	7	9	11	13	15

розрахунку зовнішньої балістики польоту куль у США та європейських країнах, без значних полігонних випробувань можливо розв'язати за допомогою підходів, зазначених у [8] та [9].

Досвід Національної гвардії України

За даними [5] військовослужбовці Національної гвардії України успішно застосовують розроблену ними кулеметну установку на пікалі з двома кулеметами ПКТ і зенітним кільцевим прицілним пристроєм для знищення дронів-камікадзе «Шахед-136» (рис. 2). Додатково в установку входить мобільна фара «Сова» для підсвічування цілі в умовах низької освітленості.

Згідно з [10] характеристики кулемету ПКТ:

- калібр 7,62 мм,
- практична скорострільність 250 пострілів на хвилину (4 постріли на секунду),

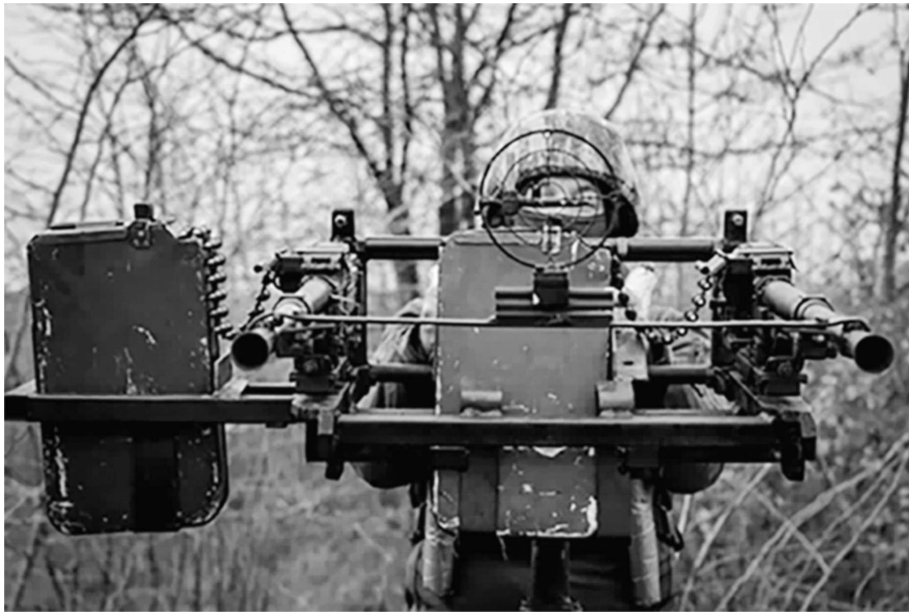


Рис. 2. Кулеметна установка [5]

- дульна швидкість 855 м/с,
- ефективна дальність стрільби 1500 м,
- кількість патронів у стрічці 250 (60 секунд безперервної роботи кулемету).

При таких характеристиках дистанція між кулями в польоті сягає 213 м. При окомірному способі визначення ракурсу і дальності до цілі ця обставина зменшує вірогідність ураження БпЛА при одночасній активації кулеметів. Як видно з фото, базова відстань між стволами ≈ 600 мм. При цьому кулеметна установка ефективніше діятиме при фланговому та скісному русі цілі, ніж при фронтальному русі малогабаритної цілі.

На основі зазначеного формуються пропозиції авторів щодо вдосконалення кулеметної установки Національної гвардії України.

1. Опрацювати можливість неодноразової активації кулеметів. Затримка активації 0,125 с.

2. При захисті об'єктів інфраструктури використовувати кулеметну установку, положення якої максимально наближене до флангового руху цілі.

3. Ввести до складу кулеметної установки пристрій визначення дистанції до дрона-камікадзе «Шахед-136» на кшталт російського пристрою «Лира» [7]. При виготовленні пристрою видимий розмір БпЛА повинен розраховуватися за формулою: $1500/D_y$ (мм), де $D_y = n100$, $n = 1, 2, 3 \dots 15$. Випередження розраховується за формулою $[0,0175 D_y]$ (корпусів БпЛА). Зауважимо, що пристрій «Лира» забезпечує найбільшу точність вимірювання дальності при фланговому русі цілі ($\sin(q) = 1$).

4. Використовувати коліаторний прицільний пристрій замість зенітного кільцевого для прискорення прицілювання. Розробити методику його «холодного» прицілювання.

Коліаторний прицільний пристрій для кулеметної установки

На конференціях, які проводились у Національній академії Національної гвардії України, автори висловлювали загальні погляди на створення перспективного коліаторного прицільного пристрою (КПП) [11, 12]. Тому тут доцільно розглянути процес автоматизації прицілювання з використанням КПП.

Як видно з формул (5) і (3), для автоматичного розрахунку кута випередження ψ необхідно знати проекцію ракурсу на горизонтальну площину q' , похилу дальність до цілі D і висоту цілі над поверхнею землі H . Останню можна розрахувати добутком $H = D \sin(\beta)$, де β – кут місця цілі.

Як було зазначено вище, величина $\sin(q')$ при візуальному спостереженні повітряної цілі із землі визначається окомірним способом за видимим скороченням довжини фюзеляжу цілі в четвертих частинах одиниці. Похила дальність до цілі D визначається лазерним далекоміром. Для відображення кута випередження ψ необхідно використовувати оптико-електронний КПП замість зенітного кільцевого прицільного пристрою і визначати кут місця цілі β . Задля цього достатньо на горизонтальній осі повороту кулеметної установки встановити потенціометр зворотного зв'язку, вихід якого з'єднати з процесором.

Останні досягнення мікроелектроніки в галузі створення рідинно-кристалічних індикаторів (наприклад матриця 8K4K D-ILA має розмір пікселя $a = 4,8$ мкм [13]) створюють передумови для розробки КПП на новій елементній базі [12]. Згідно з (5) кут ψ має максимальне значення 52,6 мрад по горизонталі при $\beta = 90^\circ$. Тоді поле зору 2ω КПП має бути не менше 6° по горизонталі.

російсько-української війни 2022–2023 років) : ВП 3-00(116) 120 : затверджені начальником Головного управління доктрин та підготовки ГШ ЗСУ 9 березня 2023 р. / Центр оперативних стандартів і методики підготовки ЗСУ, Головне управління доктрин та підготовки ГШ ЗСУ. – [Б. м. : б. в.], 2023. – 76 с.

4. Росіяни атакують міста дронами «Герань-2»: що це таке і як збити безпілотною (фото) [Електронний ресурс] // Фокус. – Режим доступу : <https://focus.ua/uk/voennye-novosti/533239-rossiyane-atakuyut-goroda-dronami-geran-2-chto-eto-takoe-i-kak-sbit-bespilotnik-foto>.

5. Бійці Нацгвардії створили установку з кулеметами ПКТ для знищення безпілотною противника [Електронний ресурс] // Національна гвардія України. – Режим доступу : <https://ngu.gov.ua/?p=12330>.

6. Мубаракшин Р. В. Прицельные системы стрельбы. Часть 1 / Р. В. Мубаракшин, В. М. Балуев, Б. В. Воронов. – М. : ВВИА им. проф. Н. Е. Жуковского, 1973. – 332 с.

7. Методика обучения ведению огня по беспилотным летательным аппаратам из стрелкового оружия / ГУ боевой подготовки ВС РФ. – М. : [ГУБП ВС РФ], 2018. – 38 с.

8. Method of Conversion for the Ballistic Coefficient of Bullets [Електронний ресурс] / I. B. Chepkov, A. V. Hurnovych, S. V. Lapyts'kyi, et al. // Strength of Materials. – 2020. – Vol. 52, issue 3. – P. 419–422. – Режим доступу : <https://doi.org/10.1007/s11223-020-00193-8>.

9. Method of Measuring the Ballistic Coefficient of Bullets [Електронний ресурс] / I. B. Chepkov, A. V. Hurnovych, S. V. Lapyts'kyi, et al. // Strength of Materials. – 2019. –

Vol. 51, issue 5. – P. 721–725. – Режим доступу : <https://doi.org/10.1007/s11223-019-00120-6>.

10. Кулемет Калашникова [Електронний ресурс] // Вікіпедія. – Режим доступу : https://uk.wikipedia.org/wiki/Кулемет_Калашникова.

11. Сенаторов В. М. Коліматорний приціл для потреб Національної гвардії України / В. М. Сенаторов, А. В. Гурнович // Службово-бойова діяльність Національної гвардії України: сучасний стан, проблеми та перспективи : збірник тез доповідей науково-практичної конференції : секція 2. Логістичне забезпечення службово-бойової діяльності Національної гвардії України: сучасний стан, проблеми та перспективи, 31 березня 2022 р., м. Харків / Національна академія Національної гвардії України. – Харків : НА НГУ, 2022 – С. 39–40.

12. Коліматорний приціл для потреб Збройних Сил і Національної гвардії України / В. М. Сенаторов, А. В. Гурнович, Б. О. Мельник, К. В. Мереж // Актуальні проблеми діяльності складових сектору безпеки і оборони України в умовах особливих правових режимів: поточний стан та шляхи вирішення : збірник тез доповідей Всеукраїнської науково-практичної конференції, 30 березня 2023 р., м. Харків / Національна академія Національної гвардії України. – Харків : НА НГУ, 2023. – С. 611–613.

13. JVC Develops 1.75-inch 8K4K D-ILA Device [Електронний ресурс] : press release // JVC. – Режим доступу : http://pro.jvc.com/pro/pr/2008/releases/JVC_Develops_1.75-inch_8K4K_D-ILA_Device_f.pdf.

DOI 10.33099/2618-1614-2023-23-4-48-56

UDC 355.4:004.056.5

V. V. Mashtalir,*Doctor of Historical Science, Professor,
Head of the Institute of Information and Communication
Technologies and Cyber Defence,
the National Defence University of Ukraine, Colonel,***V. V. Shypovskiy,***PhD Student at the Science and Technology Management Centre,
the National Defence University of Ukraine,
Lieutenant Colonel*

Analysis of the cyber domain during the Russian-Ukrainian war 2022: conclusions, recommendations, lessons learned

The Russian invasion of Ukraine demonstrated the spread of modern military operations to almost all aspects of daily life. The development of the internet and widespread use of digital technologies mean that virtually everything, from water supply to banking services, can fall into the hands of criminals and be disrupted. The article analyses events in the cyber domain related to the large-scale Russian Federation's invasion of Ukraine starting from 2014 when Crimea was annexed and armed conflict began in eastern Ukraine. It presents statistical data on cyber-attacks carried out, depicts the structure of both sides' confrontation, and describes new ways of applying cyber influence in conjunction with other dimensions of processes related to Russian occupation actions. Moreover, the article reveals changes in the targets of cyber operations depending on the political situation worldwide or the situation on the battlefield.

Key words: cyber defence, cyber resilience, information technologies, critical infrastructure, cyber operation, cyber warfare.

© V. V. Mashtalir, V. V. Shypovskiy, 2023

Introduction. Cyber-attacks on Ukraine began before the invasion. The intensity of cyber-attacks began to increase significantly in January and peaked in February. Only during 23 February 2022, Russia has attacked 19 government and critical infrastructure facilities. This was done by the same hacker group that launched the NotPetya virus in 2017 and that works for Russian military intelligence.

Cyber threats to the Ukrainian state and society can be conditionally divided into two key levels. The first – «classic» cybercrimes – both completely original and already common, they require only modern information technologies for their implementation. The second is crimes characteristic of geopolitical struggle (or such crimes at the local level that have the potential to affect the political situation of the state): hacktivism, cyber espionage and cyber sabotage. At the same time, the attack techniques in both cases show a lot in common. For example, phishing techniques can be used both for seizing citizens' funds and for the purpose of cyber espionage

Statistics and analytics. During 2022 Russian cyber-attacks against 128 targets in 42 countries have been recorded, including against targets allegedly related to aid to Ukraine [1]:

- 49% – for government structures. But there were also attacks on energy, defence and other strategic companies. Most of the attacks are against NATO countries.
- 29% of attacks were successful. A quarter of successful attacks result in stolen data. Figure 1 shows the directions that were most attacked by Russian special forces.

Since the beginning of Russia's full-scale war against Ukraine, DDoS attacks have remained among the most common types of cyberattacks used by hostile hackers [2]. Since the beginning of this year, a number of websites of state bodies and banking institutions, telecom operators, companies in the energy sector, websites of regional authorities, media, etc. have been subjected to DDoS attacks. Usually, DDoS attacks are carried out with the aim of spreading panic and destabilization. Sometimes used to hide destructive actions, that is, when a DDoS attack serves as a cover for another type of attack. However, DDoS attacks themselves do not pose a threat to personal data of citizens. It is worth knowing that hackers often use hacked devices of people to carry out DDoS attacks. Therefore, it is important to follow the basic rules of cyber hygiene, use antiviruses, update software in a timely manner, etc.

The analysis of cyberattacks on the information infrastructure of Ukraine will be expediently considered from 2014 – because it was from this year that Russia began to act beyond the borders of the information space: it was in 2014 that Russia annexed Crimea and began hybrid actions in the East of Ukraine, occupying part of Donbas.

Russian-Ukrainian Cyber War since 2014. The first attacks on information systems of private enterprises and government institutions in Ukraine were recorded during

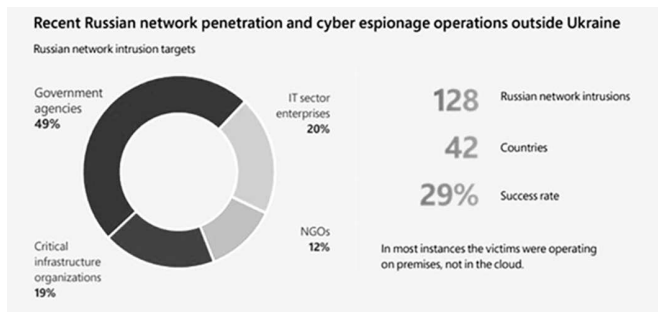


Fig. 1. Russian cyber operations outside Ukraine (source: [1])

the mass protests in 2013. The Russo-Ukrainian cyber war became the first conflict in cyberspace where a successful attack on the energy system with its disruption took place. There were attacks against the «Elections» information system during the presidential elections, numerous denial-of-service attacks, defacements, cyber espionage, and more.

On 5 March 2014, a phone call between the foreign ministers of Estonia and the EU surfaced on the Internet, containing fake information claiming that Ukrainian opposition forces were behind the sniper shootings on the Maidan Square. This viewpoint was actively promoted by Russian propaganda. In March 2014, during the early stages of Crimea's occupation, Russian intelligence services blocked communication between Ukrainian parliamentarians and the Security Service of Ukraine units in Crimea using an IP-telephone attack.

From 21 to 25 May, DDoS attacks and website hacking occurred during the presidential elections, leading to the publication of false results on the Central Election Commission's website. Despite reports of the hacking, these data were presented as real election results in Ukraine on Russian Channel One.

In June 2014, harmful programs engaged in cyber espionage, such as Turla/Uroburos/Snake, RedOctober, MiniDuke, and NetTraveler, were discovered on the servers of private companies in Ukraine and NATO countries. Analysis indicated that these programs were developed in Russia.

Since 2014, terrorist groups fighting in Donbas have been conducting signals intelligence, hacking into databases to obtain information on the locations of phones and Wi-Fi networks used by Ukrainian Armed Forces.

In October 2015, a private investigation revealed that Russian cyber espionage targeted data related to the investigation of the MH17 flight disaster, conducted by Dutch, Malaysian, Australian, Belgian, and Ukrainian authorities.

On 23 December 2015, approximately 30 substations of Prykarpattiaoblenergo were disabled using the Trojan program BlackEnergy3, which had been previously associated with Russian hackers. As a result, more than 200,000 residents of Ivano-Frankivsk Oblast were left

without electricity for a duration of one to five hours. Similar attacks also occurred on Kyivoblenergo and Chernivtsioblenergo. This was the first cyber-attack against the Critical Infrastructure of Ukraine.

On 6 December 2016, a hacker attack targeted the internal telecommunications networks of the Ministry of Finance, the State Treasury, and the Pension Fund, causing the disruption of several computers and the destruction of critical databases, leading to delays in budgetary payments amounting to hundreds of millions of hryvnias.

On 15 December 2016, Ukrainian hackers, commissioned by an unidentified individual from St. Petersburg, carried out a DDoS attack on the Ukrzaliznytsia website, completely blocking its operation for a day. The attack was believed to be aimed at stealing data on passenger transportation.

On 17 December 2016, a cyber-attack on the North Substation of Ukrenergo led to a failure in the control automation system, leaving several hours without electricity the northern part of the right-bank Kyiv and adjacent areas of the region.

On 27 June 2017, a massive cyber-attack using the NotPetya (also known as Petya.A) virus disrupted the operations of numerous Ukrainian state and private enterprises, including the Borispol airport, Ukrtelecom, Chernobyl Nuclear Power Plant, Ukrzaliznytsia, the Cabinet of Ministers, and several media outlets [3]. Figure 2 shows a screenshot of the NotPetya deface attack. It was noted on the monitors that the victim could return the encrypted data by sending the ransom to the specified address. But in reality, this option was not available, that is, the attack was an act of ordinary vandalism with the aim of destroying critical information infrastructure.

The Security Service of Ukraine (SBU) attributed the attack to Russian intelligence services.

Analysing the goals of cyber operations against the information infrastructure of Ukraine starting in 2014, the cyber troops of the Russian Federation aimed to physically destroy the state's critical infrastructure. That is why the protection of information systems of critical infrastructure objects is of critical importance during warfare.

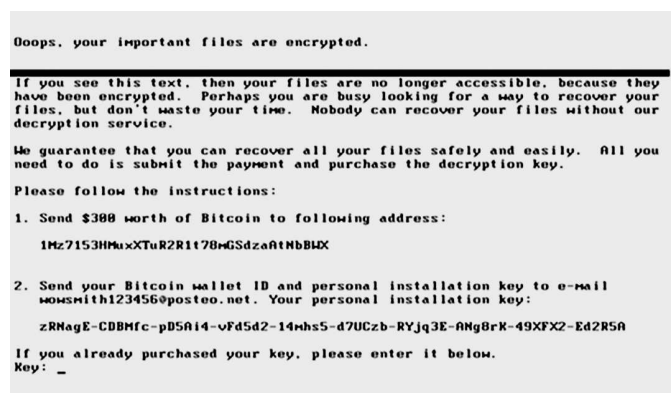


Fig.2. NotPetya virus screenshot

In 2014, the leadership of Ukraine understood that the enemy has new tools of invisible and unproven destructive influence on the country. On 27 January 2016, the National Security and Defence Council of Ukraine adopted the Cyber Security Strategy of Ukraine [4], and this became a kind of «vaccination» for how to response to new challenges.

Cyberattacks chronology in 2022. The official website of the State Service of Special Communications and Information Protection of Ukraine [5] notes the following chronology of cyberattacks since the beginning of Russia's large-scale invasion of Ukraine.

13–14 January 2022. Massive Attack on Ukrainian Government Websites. During the night of January 13 to 14, hackers launched a massive attack on Ukrainian government websites. This includes the websites of the Ministry of Education, Ministry of Foreign Affairs, Ministry of Sports, Ministry of Energy, Ministry of Agriculture, Ministry of Veterans Affairs, Ministry of Environment, State Emergency Service, and State Treasury.

The Security Service of Ukraine (SBU) together with the State Special Communications Service and Cyber Police suspect that the government websites were hacked by hacker groups associated with Russian special services. However, the National Security and Defence Council of Ukraine has different suspects and stated: «Preliminarily, we believe that the UNC1151 – a cyber espionage group associated with the Belarusian special services – may be involved in this attack.»

This attack was called a supply chain attack, meaning it was carried out through a chain of supply. The attackers compromised the infrastructure of a commercial company that had administrative access to the affected websites, allowing them to conduct the attack.

It is worth noting that all affected government websites were built on the October CMS content management system, and almost all of them were developed by a single private company. *Figure 3* shows a screenshot of an attack on Ukrainian government websites, which contains a threatening message in Russian, Ukrainian, and Polish.



Fig. 3. Deface cyberattack screenshot

The current working theory suggests a combination of three attack vectors: the supply chain attack and the exploitation of vulnerabilities in October CMS and Log4j. The attack allowed the perpetrators to modify the main pages of the websites and block access to everything else. According to the head of the State Special Communications Service, available data indicates that the cyber-attacks were well-prepared, carried out by a coordinated group of hackers, and executed at a high operational level. The attribution points to the involvement of Russian hacker groups. In 2021, there were identifications of cyber-attacks by Russian special services on a significant portion of the currently affected institutions, as stated by the head of the organization.

26 January 2022. Cyber-Attack on Ukraine.ua Website. During the night of January 26, a cyber-attack was launched on the official website of Ukraine, Ukraine.ua. As a result of the attack, the website was unavailable to users for several hours.

15 February 2022. Cyber-Attacks on Banks and Ministry of Defence Websites. The hackers took advantage of a DDoS attack on the official website of the Ministry of Defence of Ukraine, overwhelming the server's capacity with an excessive number of requests per second. It appears that they were aware that the website was protected against classical DDoS attacks, leading them to seek vulnerabilities in the site's code. As a result, the attack was effective.

The largest Ukrainian bank, Oshchadbank, also faced a DDoS attack, but their systems were well protected and operated in a normal mode. However, there was some slowdown in accessing the Oshchad 24/7 system due to increased communication channel load.

Another target was Privatbank, which experienced a DDoS attack. Although the bank's services were successfully restored, Privat24, a banking service, remained unstable for a period.

Following the attacks on banks and government websites, there was a powerful DDoS attack on the Diia (Action) portal. Initially originating from Russia and China hundreds of thousands of packets of malicious traffic per second, the attack was quickly blocked by Ukrainian experts. However, the attack resumed from servers located in the Czech Republic and Uzbekistan. Fortunately, the attack went unnoticed by Diia portal users.

In addition, the CERT-UA (Computer Emergency Response Team Ukraine) noted the occurrence of DDoS on Ukrainian bank and government website resources. Investigation, including information from partners, revealed the involvement of Mirai and Meris botnets in the attacks. The use of readily available malicious traffic from cybercriminals, known as DDoS-as-a-Service, was also considered. DNS-server-based DDoS attacks were used to prevent access to government websites in the gov.ua domain by disrupting DNS servers.

On 23 February 2022, a new series of mass DDoS attacks targeted the websites of government and banking

institutions. Some of the attacked information systems became inaccessible or operated with disruptions, leading to rerouting traffic to minimize damage. However, other sites effectively resisted the attacks and operated normally.

Phishing attacks on government authorities and critical infrastructure objects, distribution of malicious software, and attempts to breach private and public sector networks for further destructive actions also increased in tandem with the DDoS attacks.

The cybersecurity teams of various institutions, internet providers, and IT teams of critical information infrastructure objects worked around the clock to ensure the availability and integrity of information resources.

The attackers behind these cyber-attacks were blatant in their actions and used botnets for phishing campaigns and DDoS attacks. Ukrainian intelligence agencies attribute the attacks to hackers associated with the aggressor country, Russia.

On 24 February 2022, Viasat, a media company, was subjected to a massive cyber-attack, leading to disruptions in the operation of Ukrainian government websites. The incident is suspected to be connected with Russian hackers. According to SentinelOne, the cyber-attack involved the Wiper virus strain called AcidRain, which was discovered on 15 March. The virus destroys data and renders devices unusable after rebooting. The identities of the hackers behind the attack have not been established. However, researchers noted similarities between AcidRain and the VPNFilter virus, which had been linked to Russian hacking groups Fancy Bear and APT28 by the FBI.

On 25 February 2022, the State Special Communications Service and Information Protection of Ukraine reported mass phishing emails sent to the email addresses of Ukrainian military personnel on i.ua and meta.ua services. These phishing attacks targeted private mailboxes of Ukrainian military personnel and individuals associated with them. After compromising the account, the attackers downloaded the entire mailbox content using the IMAP protocol and obtained contact addresses for further distribution. The UNC1151 group, located in Minsk and consisting of officers of the Ministry of Defence of Belarus, is believed to be behind these actions.

Russian cyber war actors. According to the information available up to that point, it was believed that the Russian cybertroops operated under the umbrella of the Russian military and intelligence agencies. Here is a general overview of their structure and assigned next roles. The structure of the state cyber forces of the Russian Federation is shown in Figure 4.

Main Intelligence Agency (GRU) Cyber Units:

The GRU, known as the Main Intelligence Agency, serves as Russia's military intelligence agency. Its responsibilities include gathering and analysing intelligence and conducting cyber operations to support Russia's military objectives. GRU cyber units are highly

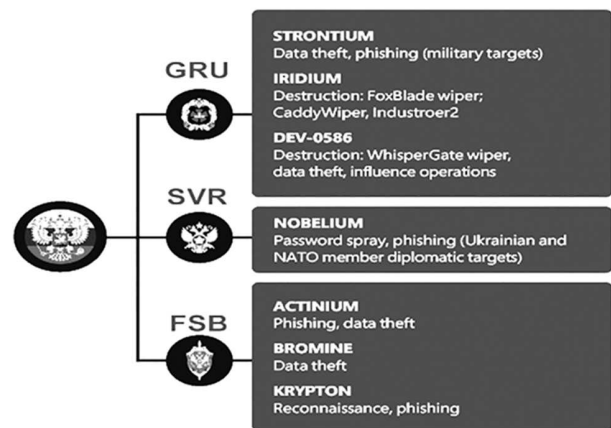


Fig. 4. Russian cyber troops structure (source: [1])

advanced and engage in offensive cyber activities, such as hacking, infiltrating networks, and conducting cyber espionage.

Federal Security Service (FSB) Cyber Division:

The FSB is Russia's domestic security agency responsible for counterintelligence, counterterrorism, and national security matters. The FSB Cyber Division focuses on carrying out cyber operations against domestic and foreign targets considered threats to Russia's national security.

Ministry of Defence Cyber Commands:

The Russian Ministry of Defence is in charge of the country's military affairs and national defence. Within the Ministry of Defence, specific cyber commands or units are likely responsible for conducting cyber operations to support military objectives and safeguard critical military infrastructure.

Presidential Executive Office:

The Presidential Executive Office plays a crucial role in Russia's governance, advising and assisting the President in policy-making and administrative matters.

While specific details may be limited, this office is believed to be involved in coordinating and directing strategic cyber efforts in alignment with Russia's broader foreign policy goals.

State-sponsored Hactivist and Proxy Groups:

Russia has faced accusations of employing state-sponsored hactivist groups or utilizing proxy groups to conduct cyber operations on its behalf. These groups may have varying degrees of affiliation with Russian intelligence agencies or government entities. They are often engaged in disinformation campaigns, propagating propaganda, and launching cyber-attacks against political opponents and other countries.

It's essential to emphasize that attributing actions in the cyber domain can be challenging, and specific

responsibilities and affiliations of various cyber units may not always be transparent. It's crucial that the landscape of cyber warfare is constantly evolving, and governments worldwide continuously adapt their cyber capabilities and organizational structures in response to emerging threats and challenges.

To understand the forces and means that effectively oppose the Russian invaders and protect the Ukrainian national cyberspace, it will be important to understand the directions of work of the elements of the National Cyber Security System of Ukraine.

National Cybersecurity System of Ukraine. For a broad understanding of Ukrainian forces and means of defence in cyberspace, it is necessary to consider the National Cyber Defence System, the elements of this system and the features of its application.

The National Cybersecurity System is a combination of cybersecurity assurance entities and interconnected measures of organizational, legal, political, socio-economic, scientific-technical, law enforcement, defence, informational, and educational nature, as well as measures for information protection and cybersecurity.

The main entities of the national cybersecurity system are the State Special Communications and Information Protection Service of Ukraine, the National Police of Ukraine, the Security Service of Ukraine, the Ministry of Defence of Ukraine, the General Staff of the Armed Forces of Ukraine, intelligence agencies, and the National Bank of Ukraine [6].

Ukraine has taken major steps to improve its cyber resilience in recent years. The creation of the National Cybersecurity Coordination Centre in 2016 and proposed updates to cybercrime laws align with international best practices. Ukraine's close cooperation on cyber defence with other nations also enhances its capabilities [7].

However, Ukraine's National Cybersecurity Strategy identifies ongoing cybersecurity threats. These include Ukraine's outdated electronic communications infrastructure, insufficient critical infrastructure protections, unsystematic cyber defences, and ineffective security sector activities against cyber threats. Additional challenges are inadequate coordination and information sharing among Ukrainian cybersecurity entities. Overall, while Ukraine has made progress, vulnerabilities remain due to outdated systems, uneven protections, and uncoordinated efforts. Further modernization, strengthened critical infrastructure

defences, systematic approaches, enhanced security sector activities, and improved collaboration are needed to bolster Ukraine's cyber resilience.

Cyber warfare evolution. In [8], in order to analyse what has contributed to the success of Ukraine's cyber defence, Russia's approach to offensive operations and the tactical adaptations its cyber forces have made to operate under conditions of war were studied. The trends of changing directions of target selection by the Russian special services were successfully reflected. *Figure 5* shows the main phases of cyber warfare during 2022.

Examining Russia's cyber offensive in parallel with its conventional military campaign revealed significant correlations between the two. Throughout each phase, the pattern of cyber operations and their impact on Ukraine's Critical infrastructure underwent adjustments that aligned with Russia's evolving war objectives. Russian cyber actors displayed a discernible evolution in their operational priorities, target selection, and tactics, adapting to the shifting dynamics and challenges in the highly contested operating environment [8].

The initial phase of the war showcases Russia's utilization of cyber operations to create shock and surprise, complementing its invasion force. Subsequent phases shed light on Russia's deployment of cyber units in a prolonged war of attrition. Monitoring these changes chronologically provides a unique perspective on the versatile role that cyber operations might assume in future conflicts. It also highlights the specific obstacles Russia encountered in wielding cyber power when rapidly changing operational requirements were driven by events on the ground. Overall, studying Russia's cyber offensive through different phases offers a comprehensive understanding of its strategic intentions and the multifaceted challenges posed by cyber warfare in complex and fast-paced military scenarios. Let's consider the phases of cyber operations and analyse the state in other dimensions for the time intervals indicated in the phases.

Phase 1: Active Preparation (March 2021 – 23 February 2022). During the March 2021 phase, Russian cyber groups escalated efforts to gain access to critical infrastructure networks in Ukraine. Russia's cyberattacks on Ukraine aligned with its military escalation, foreshadowing the invasion. As Russian troops amassed near Ukraine's borders, Russian intelligence cyber units reactivated old intrusions of Ukrainian networks dating back to 2019. The GRU cyber

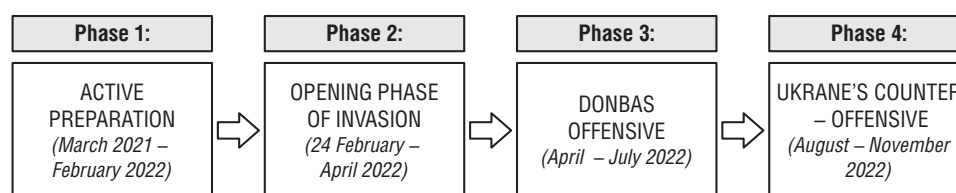


Fig. 5. Cyber warfare phases during 2022 (source: [8])

warfare branch leveraged these dormant access points to launch attacks. The cyber operations employed relatively basic tactics like stealing login credentials, brute-force hacking, and exploiting known security flaws. The goal was to degrade Ukrainian systems and wear down cyber defenders, setting the stage for larger cyberattacks once the planned invasion commenced. Rather than advanced cyber techniques, Russia relied on rudimentary methods to disrupt Ukraine before the kinetic phase. This exemplified Russia's cyber-enabled hybrid warfare strategy, coordinating cyber and military aggression to overwhelm the adversary. However, this move proved a miscalculation, exposing GRU activities prematurely, serving as an early warning for global cyber defenders over a month before the invasion. Russia's invasion anticipated swift success, but the cyber operation drew heightened attention and vigilance from the global cybersecurity community instead [8].

There is a large amount of evidence that Russian hackers were preparing for the invasion in advance, namely from 2021. Consider the report of the company Microsoft for 2021. Data from Microsoft reveals Russia's growing cyber threat. In 2021, over half of all nation-state cyberattacks observed by Microsoft originated from Russia. Moreover, Russian cyber operations were becoming more successful – their compromise rate rose from 21% in 2020 to 32% in 2021. Russian actors primarily targeted government agencies, comprising 53% of attacks versus just 3% in 2020. Their focus was intelligence gathering, especially targeting agencies handling foreign affairs, national security, and defence. The top 3 countries Russia cyber actors struck were the United States, Ukraine, and the United Kingdom [9].

Overall, these statistics highlight the escalating scale, effectiveness, and strategic nature of Russian cyber campaigns against critical government systems and Western nations. This fact also indicates that the Russian foreign intelligence services anticipated help to Ukraine from Great Britain and the United States after the large-scale Russian invasion.

Phase 2: Phase of Invasion (24 February – April 2022). The preparatory activities carried out during Phase 1 were extensively leveraged to support Russia's initial campaign aimed at swiftly capturing Kyiv and toppling Ukraine's democratically elected government. Offensive cyber operations (OCOs) were instrumental in disrupting essential elements of Ukrainian society as part of a long-standing campaign to portray Ukraine as a failed state incapable of recovering or maintaining critical services [8].

At the onset of the invasion, Russia aggressively exploited its pre-established access to Ukrainian networks, focusing primarily on high-priority strategic targets within Ukraine. This opening onslaught involved the use of more advanced destructive cyber tools to disrupt command and control (C2) infrastructure, weaken Ukraine's resolve, and create favourable conditions for the success of the invading

forces. The intensity of these early cyber operations aligned with Russia's approach of using cyber disruptions as a precursor to military actions and the strategic value of leveraging pre-positioned cyber capabilities at the outset of a conflict [8].

During this phase, Russia's cyber campaign was largely oriented towards counter-value targets, systematically disrupting the Ukrainian government's ability to function and communicate with the public, as well as undermining critical infrastructure functions in civilian areas. For example, HermeticWiper targeted numerous organizations across a broad spectrum of Ukraine's critical infrastructure sectors, including government, aviation, IT, energy, defence industry, agriculture, and financial services. In addition to using more potent cyber tools, Russia also employed less sophisticated ones to disrupt critical infrastructure networks in government, financial services, and media organizations [8].

The experience of cyber defence measures on the part of Ukraine indicates the need for special protection of critical infrastructure objects. The study [10] highlights the most common approaches to assessing the level of cyber protection of information systems, which have a wide range of applications in different countries of the world, and developed a methodology that provides the largest number of solutions. The system of indicators of cyber resilience of information systems of critical infrastructure objects, proposed in [10] provides opportunities for a more qualitative and effective assessment of the level of cyber protection and allows for a comprehensive assessment of cyber resilience of information systems, taking into account various technical and organizational aspects of critical infrastructure information protection. An improved method of factor analysis of information risks for assessment and management of information risks in critical infrastructure systems is given in [11].

The Russian special services had high hopes for Phase 2, as evidenced by the large amount of effort invested immediately before the invasion. Let's consider the relationship between cyber operations by the Russian Federation and key political events related to the Russian government (*Figure 6*).

Despite extensive planning, Russia struggled to sustain its initial intensity of cyberattacks on Ukraine beyond the first week of the war. Russia's cyber operations paused for an extended period after its blitz on Kyiv stalled, forcing a shift in military strategy. It appears Russian cyber units rapidly lost access to Ukrainian systems, hampering efforts to maintain nonstop effects after the initial onslaught. Consequently, later cyberattacks became more tactical and opportunistic as planners hastily leveraged any new network access. Defensive actions by Ukraine and partners from late 2021 onward further degraded Russia's attack capabilities, revealing a disconnect between the GRU's envisioned phase 1 strategy and actual execution [8].

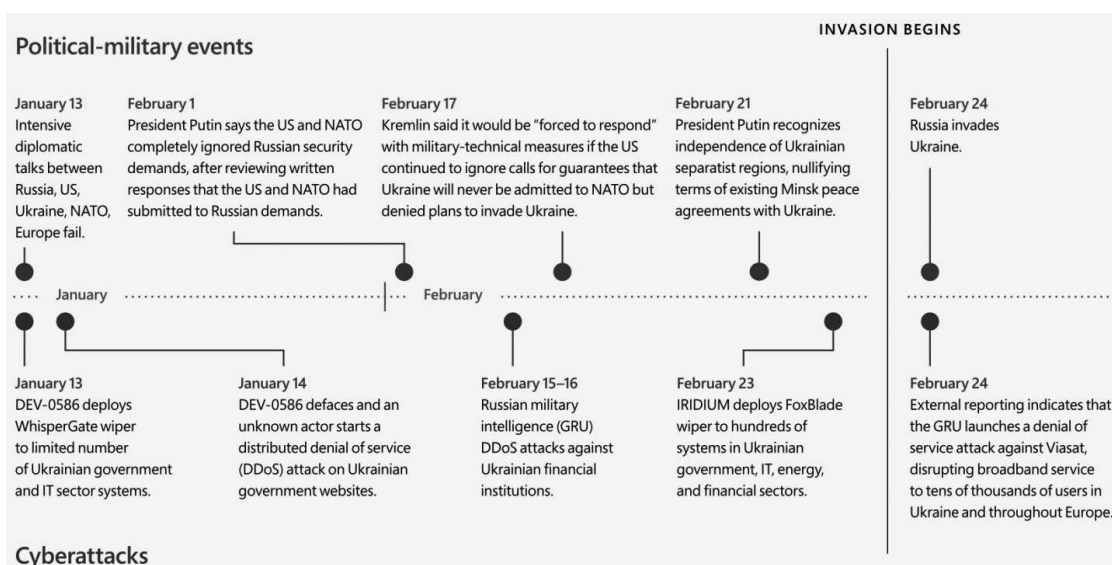


Fig. 6. Political-military events/Cyber-attacks (source: [12])

Analysis of phase 2 prerequisites shows Russian cyberattacks clearly adapted based on changing conditions in Ukraine and globally. This exemplifies Russia synchronizing cyber operations with political developments to maximize its war impact. Despite meticulous preparation, Russia's cyber units failed to sustain the intensity of early operations due to defenders' actions and Russia's military setbacks. This forced a reactive, makeshift approach relying on fleeting access, underscoring the importance of resilient cyber defences to frustrate an aggressor's designs.

Phase 3: Donbas Offensive (April – July 2022). Following Russia's unsuccessful initial invasion and pivot to eastern Ukraine, destructive cyberattacks on Ukrainian critical infrastructure declined. Russia refocused its cyber capabilities to enable the impending Donbas offensive.

Rather than continuing disruptive strikes on Ukrainian systems, Russia conserved its cyber resources. This likely aimed to support military operations in eastern Ukraine. By curtailing broad cyberattacks and reserving its most potent cyber weapons, Russia prepared its cyber arsenal to complement the ground assault on Donbas. The shift in cyber strategy indicates Russia learned from the failed Kyiv blitz. By aligning cyber with realistic military plans, Russia hoped to avoid overextending its cyber capabilities early on. This adaptation highlights Russia's efforts to better integrate cyber operations with its larger strategic aims in Ukraine.

GRU hackers used Industroyer2 to attempt power outages in eastern Ukraine, redirecting attention from Kyiv. Reasons for reduced cyber disruptions are unclear. It could be due to the conflict narrowing, making cyber less strategic. Russian cyber forces might have transitioned to intelligence gathering, away from frontline. Aggressive earlier phase took a toll on Russian cyber forces. Challenges in sustaining operations during invasion's second phase

emerged. Russia's strategic priorities adapted, targeting Eastern European countries and defence organizations. Simple tactics like phishing, cookie theft, and exploiting known vulnerabilities persisted. Russia incorporated more intermediary tools from criminal markets. Destructive capabilities narrowed, with CaddyWiper emerging as preferred wiper [8].

During phase 3, experts observed a change not only in the intensity of cyber operations, but also in the ways and means of cyber-attacks, which indicates, first of all, a change in the managers of cyber operations against the Ukrainian information infrastructure and the infrastructure of partner countries [13].

Russia's cyber arsenal expanded, but capabilities focused. Adaptive learning demonstrated GRU's aptitude for prolonged conflict. Russia built up cyber forces and refined tools, concentrating them on key targets. Through training, GRU gained proficiency in effectively deploying cyberweapons, integrating them into military strategy. This underscores the systemic nature of the threat. Countering requires robust security and flexible defence adjustment. Critically important are investments in personnel, decision-making, and institutional learning.

In summary, Russia methodically honed its cyber capabilities for wartime application, enabling integrated cyber-kinetic operations. This systemic threat demands durable safeguards and adaptive preparedness. Vital priorities are workforce development, streamlined decisions, and organizational learning to match Russia's focused cyber advances.

Phase 4: Ukraine's Counter-offensive (August – November 2022). Russia continued to adjust its operations to address previous challenges in balancing access and action. Russian cyber units exhibited a continued diversification of methods for gaining access to Ukrainian critical infrastructure.

Moreover, they deepened their longstanding preference for commodity tools to quickly supplement their arsenals, alongside internal development resources. Starting in October 2022, there was an increase in reported network attacks, suggesting a more prepared and reinvigorated Russian cyber program compared to the summer period. Particularly noteworthy was the surge in Russian network attacks against energy, water, and logistics organizations, coinciding with deliberate targeting of Ukraine's energy infrastructure using missiles and loitering munitions. This coordination indicated a strategy to intensify cross-domain pressure and deprive civilians of essential services as the winter season approached [8].

Summarizing the 4 phases of 2022, it was found that just like resistance on the battlefield, Russia did not expect resistance in cyberspace from the components of the National Cyber Security System of Ukraine and volunteers of the civilian sector. Analysing the data of the Cyber Incidents Response Operational Centre of the State Cyber Protection Centre of the State Service of Special Communication and Information Protection of Ukraine [14], it is possible to say that Ukraine is now in the phase 5 – Cyber war of attrition. Since the beginning of 2023 (compared to the 4th quarter of 2022), there has been a decrease in the total number of cyberattacks organized by pro-Russian hacktivist groups, but their systematicity and intensity continues to be on a high level. However, Kremlin intensified information operations to justify the unprovoked invasion of Ukraine creating conditions for a protracted war in Ukraine, so there is no fundamental reason to believe that the downward trend in the number of cyber-attacks targeting Ukrainian organizations of various forms of ownership and industries will continue.

Conclusions and Lessons learned.

We have one enemy, and this enemy is well-prepared for future strikes. They are ready to carry out cyber-attacks on democratic countries. To effectively counter Russian hackers, we need to concentrate efforts on strengthening cyber resilience and preventing aggression in cyberspace. It is crucial to enhance rapid response teams, work on standards, build mutually beneficial partnerships, and establish joint cyber aggression response teams.

The main goal is to raise awareness about the threats. Digital security and cyber hygiene must become part of everyday life for both ordinary citizens and leaders.

Security standards serve as the barrier between us and the enemy. This barrier exists in every smartphone, computer, registry, and company system.

Russia's cyberattacks on Ukraine show how cyber can enable military and political goals. Russian criminal groups coordinate closely with intelligence agencies like the GRU, FSB, and military. Objectives are not just extortion, but collecting intelligence on infrastructure and citizens to disrupt systems and undermine trust in government.

Russia deliberately targets civilians, confirming its global cyber threat as a rogue state. Sanctions to isolate Russia from the internet are warranted.

With the war ongoing, critical infrastructure protection must be a top priority to defend civilians, especially in winter. Cyber threats are the main danger to NATO members, who have increased cyber spending and policymaking in response. Critical infrastructure cyber resilience remains vital. All of Ukraine's cyber defences must prioritize securing critical systems.

Overall, Russia weaponizes cyber to support kinetic operations and political aims. Close coordination between Russian state hackers, military, and criminals make cyberattacks a systemic threat. Protecting civilians and critical systems is imperative, requiring global isolation of Russia from the internet, together with resilient cyber defences, especially of critical infrastructure of Ukraine and partner countries.

References

1. Defending Ukraine: Early Lessons from the Cyber War [Електронний ресурс] // Microsoft. – Режим доступу : <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK>.
2. Lewis J. A. Cyber War and Ukraine [Електронний ресурс] / J. A. Lewis // SCIS. – Режим доступу : <https://www.csis.org/analysis/cyber-war-and-ukraine>.
3. Пшета́чник Я. Війна Росії проти України: хронологія кібератак [Електронний ресурс] / Я. Пшета́чник, С. Тарпова ; Дослідницька служба Європейського парламенту // European Parliament. – Режим доступу : [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI\(2022\)733549_XL.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf).
4. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс] : Указ Президента України № 96/2016 від 15 березня 2016 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/96/2016#n2>.
5. News [Електронний ресурс] // State Service of Special Communications and Information Protection of Ukraine. – Режим доступу : <https://cip.gov.ua/en/news>.
6. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] : Закон України № 2163-VIII від 5 жовтня 2017 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
7. Spinu N. Ukraine Cybersecurity Governance Assessment [Електронний ресурс] / N. Spinu // DCAF. – Режим доступу : <https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf>.
8. Black D. Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences [Електронний ресурс] / D. Black // IISS. – Режим доступу : <https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/03/russias-war-in-ukraine-examining-the-success-of-ukrainian-cyber-defences.pdf>.
9. Burt T. Russian cyberattacks pose greater risk to governments and other insights from our annual report

[Електронний ресурс] / Т. Burt // Microsoft. – Режим доступу : <https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021>.

10. Шиповський В. В. Система показників оцінювання кіберстійкості інформаційних систем об'єктів критичної інфраструктури [Електронний ресурс] / В. В. Шиповський // Захист інформації. – 2023. – Том 25, № 1. – С. 37–45. – Режим доступу : <https://doi.org/10.18372/2410-7840.25.17597>.

11. Shypovskiy V. Enhancing the factor analysis of information risk methodology for assessing cyberresilience in critical infrastructure information systems [Електронний ресурс] / V. Shypovskiy // Political Science and Security Studies Journal. – 2023. – Vol. 4, No 1. – P. 25–33. – Режим доступу : <https://doi.org/10.5281/zenodo.7876556>.

12. An overview of Russia's cyberattack activity in Ukraine [Електронний ресурс] : Special Report: Ukraine // Microsoft. – Режим доступу : <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd>.

13. Cyber Threats Snapshot, the latest report on attacks, vulnerabilities and threat actors in Q2 2022 [Електронний ресурс] // Leonardo. Cyber & Security. – Режим доступу : <https://cybersecurity.leonardo.com/en/news-and-stories-detail/-/detail/cyber-threats-snapshot-q2-2022>.

14. Q3 2023 Report [Електронний ресурс] // State Cyber Protection Center of the State Service of Special Communications and Information Protection. – Режим доступу : <https://scpc.gov.ua/en/articles/327>.

A. P. Kazmirchuk, Doctor of Medical Sciences, Professor, Commander of the Medical Forces of the Armed Forces of Ukraine, Major General MS,

V. L. Savytskyi, Doctor of Medical Sciences, Professor, Chief of the Ukrainian Military-Medical Academy, Brigadier General MS,

V. O. Zhakhovskyi, Candidate of Sciences in Public Administration, Associate Professor, Leading Researcher at the Research Institute of Military Medicine, the Ukrainian Military-Medical Academy,

V. H. Livinskyi, Candidate of Medical Sciences, Leading Researcher at the Research Institute of Military Medicine, the Ukrainian Military-Medical Academy

Methodological approaches to the resource supply of the Medical Forces of the Armed Forces of Ukraine on the basis of defence planning

The article, based on the analysis of the activities of the Medical Forces of the Armed Forces of Ukraine, developed and proposed methodological approaches to determining the need for the amount of resources for proper medical support of the Armed Forces of Ukraine in the conditions of modern armed conflicts and the full-scale armed aggression against Ukraine, which should be based on the principles of defence planning.

It was established that the resources for the medical support of the Armed Forces of Ukraine have two components: the own resources of the Medical Forces and resources and services from the state health care system and other ministries and agencies (the economy of Ukraine).

The main factors that have a determining influence on the methodology and procedure for calculating the amount of necessary resources for the medical support of the Armed Forces of Ukraine are defined and proposed.

Key words: medical support, Medical Forces of the Armed Forces of Ukraine, resources of the medical support system of the Armed Forces of Ukraine, defence planning.

A. V. Sliusarenko, Doctor of Historical Sciences, Professor, Deputy Commandant for Academic Affairs, the National Defence University of Ukraine, Colonel,

V. M. Telelym, Doctor of Military Sciences, Professor, Professor at the National Security and Defence Strategy Department, the National Defence University of Ukraine,

A. M. Zelnytskyi, Candidate of Pedagogical Sciences, Professor, Leading Researcher at the Centre for Military and Strategic Studies, the National Defence University of Ukraine,

O. A. Zabolotnyi, Candidate of Military Sciences, Associate Professor, Leading Researcher at the Centre for Military and Strategic Studies, the National Defence University of Ukraine

Quality assurance for professional military education: definition of concepts and monitoring of the current state

The article analyses and clarifies individual components of the conceptual and categorical system in the field of quality assurance for professional military education (PME) in Ukraine, proposes the structure of PME quality assurance system, indicators for assessing its condition, and also considers approaches to monitoring the quality of PME, taking into account domestic experience and experience of NATO member countries.

Key words: higher education, professional military education, quality assurance, quality monitoring, quality guaranteeing.

O. V. Safronov, Doctor of Technical Sciences, Professor, Leading Researcher at the Centre for Military and Strategic Studies, the National Defence University of Ukraine,

B. Y. Semon, Doctor of Technical Sciences, Professor, Chief Researcher at the Science and Technology Management Centre, the National Defence University of Ukraine,

O. M. Nedilko, Candidate of Technical Sciences, Associate Professor, Leading Researcher at the Science and Technology Management Centre, the National Defence University of Ukraine

A method for estimation of the maximum level of oscillations of aerodynamic control surfaces of supersonic aircraft under transonic flutter

The article proposes a method for estimation of the maximum level of oscillations of the aerodynamic control surfaces of supersonic aircraft under transonic flutter, according to which the level of oscillations of the control surfaces is determined from the condition of comparing their excited hinge moments and hinge moments from aerodynamic and structural damping forces.

The method can be recommended for a preliminary approximate assessment of the maximum level of oscillations of aerodynamic control surfaces when conducting transonic flutter studies. The feasibility of the proposed method is confirmed by comparing the results of the calculations obtained using this method with the results obtained in experimental studies.

Key words: mathematical model, oscillations, aerodynamic control surface, supersonic aircraft, safety, Mach number, transonic flutter, maximum level of oscillations.

S. V. Svieshnikov, Candidate of Technical Sciences, Senior Researcher, Leading Researcher at the Centre for Military and Strategic Studies, the National Defence University of Ukraine,

V. P. Bocharnikov, Doctor of Technical Sciences, Professor, Chief Researcher at the Centre for Military and Strategic Studies, the National Defence University of Ukraine

Use of artificial intelligence methods for solving scientific problems in the defence area

In the article, the authors at the level of conceptual models demonstrate the feasibility of artificial intelligence methods to solve applied scientific problems that take place in the field of security and defence.

Key words: artificial intelligence, fuzzy sets, fuzzy measures, neural networks, estimation, classification, clustering, forecasting.

V. M. Senatorov, Candidate of Technical Sciences, Associate Professor, Senior Researcher, the Central Research Institute of Armaments and Military Equipment of the Armed Forces of Ukraine,

A. V. Hurnovych, Doctor of Technical Sciences, Professor, Leading Researcher, the Central Research Institute of Armaments and Military Equipment of the Armed Forces of Ukraine,

B. O. Melnyk, Candidate of Technical Sciences, Senior Researcher, Head of Research Department, the Central Research Institute of Armaments and Military Equipment of the Armed Forces of Ukraine, Colonel,

A. V. Kuchynskyi, Candidate of Technical Sciences, Senior Researcher, Doctoral Student, the Central Research Institute of Armaments and Military Equipment of the Armed Forces of Ukraine, Colonel

Application of small arms to destroy the Shahed-136 kamikaze drone

The information space provides recommendations for lead corrections when firing at the Shahed-136 kamikaze drone, which vary significantly depending on the data. These contradictory data determined the purpose of the article – the development of a technique for calculating the lead, with the following verification of recommendations for firing kamikaze drones of the Shahed-136 type with small arms. In the article, on the basis of the developed theory of the eye aiming

method, the verification of the known recommendations was carried out. The verification showed that the values of corrections for the lead recommended in the sources do not differ significantly from the verification data at a short distance to the target and differ significantly at a long distance. This is explained by not taking into account the ballistic function. Recommendations were given concerning the lead corrections when using small arms that are in service with the Armed Forces of Ukraine, taking into account the ballistic function. The article includes proposals to improve a machine gun system, which is currently successfully used by the soldiers of the National Guard of Ukraine, and to create a future sighting system for it.

Key words: Shahed-136, small arms, lead, aiming device.

Машталіп В. В., доктор історичних наук, професор, начальник інституту інформаційно-комунікаційних технологій та кібероборони, Національний університет оборони України, полковник,
Шиповський В. В., ад'юнкт науково-методичного центру організації наукової та науково-технічної діяльності, Національний університет оборони України, підполковник

Аналіз подій у кіберпросторі у процесі російсько-української війни 2022 року: висновки, рекомендації, засвоєні уроки

Російське вторгнення в Україну продемонструвало поширення сучасних бойових дій майже на всі аспекти повсякденного життя. Розвиток інтернету та масове розповсюдження цифрових технологій означають, що буквально все – від водопостачання до банківських послуг – може потрапити до рук злочинців і припинити працювати. У статті аналізуються події в кіберпросторі, пов'язані з широкомасштабним вторгненням Російської Федерації в Україну, починаючи з 2014 року, коли було анексовано Крим і почалися бойові дії на сході України. Наведено статистичні дані здійснених кібератак, показано структуру обох сторін протистояння та описано нові способи застосування кібервпливів у поєднанні з іншими вимірами процесів, пов'язаних з окупаційними діями РФ, а також розкриті зміни цілей кібероперацій в залежності від політичної ситуації у світі або від ситуації на полі бою.

Ключові слова: кіберзахист, кіберстійкість, інформаційні технології, критична інфраструктура, кібероперація, кібервійна.

Основні вимоги до оформлення статей, які подаються до журналу «Наука і оборона»

Журнал приймає для опублікування статті українською або англійською мовами. Анотації статей подаються українською та англійською мовами.

Журнал «Наука і оборона» включений до категорії «Б» наукових фахових видань України (наказ Міністерства освіти і науки України № 409 від 17 березня 2020 р.).

Спеціальності, за якими видання публікує наукові праці:

253 – Військове управління (за видами збройних сил);

254 – Забезпечення військ (сил);

255 – Озброєння та військова техніка;

256 – Національна безпека (за окремими сферами забезпечення і видами діяльності);

263 – Цивільна безпека.

Подані авторами статті повинні за змістом відповідати тематиці журналу та вимогам щодо опублікування наукових статей. Передусім приймаються матеріали, в яких викладені результати наукових досліджень, спрямованих на розв'язання проблем, що мають важливе оборонне значення, статті, які містять нові теоретичні ідеї, принципи, концепції, моделі, спрямовані на пояснення певних явищ і процесів у галузі національної безпеки і оборони та прогнозування їх розвитку. Також приймаються до опублікування статті практичного змісту, які висвітлюють актуальні питання національної безпеки і оборони, науково-методичні та оглядові статті, інформаційні повідомлення про наукові новини і події.

Рукопис статті повинен бути підготовлений з використанням комп'ютера і подається до редакції в електронному вигляді. Для цього автори можуть скористатися своїми обліковими записами, попередньо зареєструвавшись на сайті журналу (<http://nio.nuou.org.ua>), або надіслати статтю на електронну пошту редакції журналу (nio2017@ukr.net).

Загальний обсяг рукопису разом з графічними матеріалами не повинен перевищувати 20 сторінок у форматі паперу А4. Поля сторінок, мм: зліва – 30, справа – 10, зверху та знизу – 20. Сторінки мають бути пронумеровані.

Основний текст статті друкується шрифтом Times New Roman чорного кольору прямого накреслення через півтора міжрядкові інтервали кеглем 14. Допускається авторські акценти виділяти напівжирним шрифтом або курсивом.

На першій сторінці рукопису розміщуються індекс УДК, назва статті, анотація, перелік ключових слів і далі текст статті. Обсяг анотації – у межах 120–150 слів, включаючи ключові слова.

У кінці статті наводиться перелік джерел, на які є посилання у тексті статті. Бібліографічні описи джерел у переліку оформлюються згідно з ГОСТ 7.1:2006. Нумерація джерел – відповідно до порядку появи їх у тексті статті.

Рисунки, таблиці, формули, посилання оформлюються відповідно до ДСТУ 3008:2015.

Ілюстрації, виконані в окремих графічних редакторах, подаються як у середині тексту, так і в окремих файлах, створених цими редакторами.

Для забезпечення гарантій сліпого рецензування відомості про авторів у файлі статті не наводяться. У разі подання статті на сайті журналу ці відомості необхідно занести у відповідні поля форми подання. Якщо стаття надсилається до редакції електронною поштою, їх необхідно розмістити в окремому файлі. Відомості про авторів надаються за формою: прізвище, ім'я та по батькові, науковий ступінь та вчене звання, найменування посади та місце роботи, військове звання, почесні звання, ідентифікатор ORCID, інформація для зворотного зв'язку (телефонні номери, адреса електронної пошти).

Про журнал «Наука і оборона»

Науково-теоретичне та науково-практичне видання «Наука і оборона» було започатковане з огляду на загальну потребу суспільства, державних діячів, політиків, учених, військових – усіх, хто опікується питаннями національної безпеки та оборони і професійно працює в цій сфері, – у друкованому засобі масової інформації, на сторінках якого обговорювалися б актуальні проблеми воєнної політики й реформування оборонної галузі держави та публікувалися б результати наукових досліджень з питань воєнної безпеки України, з воєнно-теоретичних і військово-технічних питань.

Часопис видається на громадських засадах. Найміцнішою його опорою в нелегкий час становлення були читачі та автори. Редакційна колегія сподівається на Вашу подальшу, шановні друзі, підтримку діяльності журналу «Наука і оборона», яка має на меті:

- сприяння створенню необхідного науково-теоретичного підґрунтя для постановки та розв'язання завдань військового будівництва шляхом опублікування

інформації щодо результатів основних напрямів наукових досліджень, які стосуються оборонної сфери;

- сприяння обговоренню нагальних питань реформування оборонної сфери всіма, хто опікується питаннями національної безпеки та оборони і професійно працює в цій галузі;

- поширення воєнно-наукових знань;

- сприяння підвищенню професійного рівня військово-вослужбовців Збройних Сил України та інших військових формувань, утворених згідно із чинним законодавством України.

Статті до друку відбираються з урахуванням результатів рецензування членами редакційної колегії або зовнішніми фахівцями. Передусім приймаються матеріали, в яких на підставі виконаних авторами досліджень розв'язано проблему, що має важливе оборонне значення.

Видання розповсюджується за передплатою.

Редакційна колегія може мати точку зору, відмінну від поглядів авторів.

**Видання розповсюджується за передплатою.
Передплата здійснюється у поштових відділеннях.
Передплатний індекс 74303.**

**Поточні та попередні номери журналу можна замовити у видавництві за адресою:
stylos.publish@gmail.com**

**Електронні версії попередніх випусків журналу «Наука і оборона»
можна знайти на веб-сторінці журналу: <http://nio.nuou.org.ua>,
а також на сайті Національної бібліотеки України ім. В. І. Вернадського: www.nbuv.gov.ua**

Усі права застережені.
Переклад і передрук – лише за згодою авторів і редакції.
Адреса редакції:
03049 Київ, Повітрофлотський проспект, 28.
Тел.: (044) 271-08-91, (067) 790-23-22, (066) 362-79-50.
E-mail: nio2017@ukr.net.
<http://nio.nuou.org.ua>.
Ідентифікатор медіа R30-01599.

© Національний університет оборони України, 2023

Підп. до друку 16.01.2024 р.
Формат 60х90/8. Папір офс. Друк офсет.
Ум. друк. арк. 7,5. Обл.-вид. арк. 7,5.

Видавничий дім «Стилос».
04080, Київ, вул. Оленівська, 8, к. 2.
Тел.: (050) 331-85-03.
E-mail: stylos.publish@gmail.com.
<http://www.stylos.com.ua>.
Свідоцтво про внесення
до Державного реєстру суб'єктів видавничої справи
України ДК № 1465 від 13.08.2003 р.