

## Досвід побудови системи ISTAR в АТО, особливості впровадження та перепони на шляху до підвищення бойової ефективності вогневих підрозділів

**Резюме.** У статті наведено приклад побудови й інтеграції системи ISTAR у мережоцентричну модель управління підрозділами в сучасному військовому конфлікті. Цей досвід є актуальним у контексті невідворотності зміни підходів до управління військами і необхідності підвищення бойової ефективності підрозділів України в протистоянні військовій агресії.

**Ключові слова:** цикл розвідки, цикл прийняття рішення, сенсори, мережа, поширена інформація, ситуаційна обізнаність, вимоги до інформації, намір командира, самосинхронізація.

**Постановка проблеми.** Перехід від застарілих концепцій управління військами до більш сучасних і ефективних в Україні припав на час відбиття військової агресії сусідньої держави і тому, з одного боку, задача прискорення такого переходу стоїть на найвищому державному рівні, а з іншого боку є життєвим інтересом кожного учасника антитерористичної операції (АТО) на тактичному рівні.

Управління процесами у військовій сфері не має бути менш прогресивним ніж в економіці. При цьому в прогресивному світі, включно з Україною, перехід від планової (централізованої) моделі економіки до ринкової (вільної) остаточно відбувся через доведену ефективність останньої. В умовах планової економіки управління всіма процесами здійснювалось виключно з єдиного центру, що призводило до значних заторів у кожній ланці управління і, врешті-решт, до втрати можливості своєчасно реагувати на внутрішні збої та вплив зовнішніх факторів, а, як наслідок, до неадекватності стану системи реальності. На противагу, ринкова економіка існує на принципах взаємодії кожного учасника ринку, коли коригування процесів системи відбувається на основі саморегуляції, що дає змогу тримати систему адекватною ситуації в кожній взятій відрізок часу без втрати контролю на будь-якій ділянці системи. Кожний учасник ринку є сенсором, стан якого враховується на фондових ринках і регулює систему в міру свого масштабу в мережі, яку А. Сміт назвав “невидима рука ринку”.

У 90-х роках ХХ ст. у провідних країнах світу почався перехід від централізованого управління військами до мережоцентричного (нецентралізованого), що передбачає об’єднання в реальному часі в єдину мережу всіх учасників бойового простору: джерела інформації, органи управління і засоби ураження.

У перші роки незалежності український військовий сектор програв революційну комунікаційну революцію, яка сталась у світі, але зараз управління військами має всі можливості підвищити бойову ефективність за рахунок досягнення інфокомунікаційної переваги. Користуючись новітніми розробками телекомунікаційних та інструментальних засобів, БПЛА, процедур збору, аналізу і розповсюдження розвідданих, протягом більш ніж 1000 днів антитерористичної операції тисячі тактичних підрозділів на лінії зіткнення здобувають досвід в унікальній асиметричній війні 4-го покоління.

Спираючись на підтримку провідних країн світу, Україна має можливість на державному рівні впровадити цілі концепції та розробити оновлені доктрини у військовій сфері, враховуючи як досвід власних підрозділів, здобутий за час АТО, так і доробки армій країн НАТО, які на сьогодні є незаперечними лідерами в ефективності застосування військ.

**Аналіз останніх досліджень і публікацій.** Однією з концепцій мережоцентричних операцій є ISTAR (Intelligence, surveillance, target acquisition, and reconnaissance), яка в доповіді комітету з оборони Палати громад Великої Британії 2010 р. названа “серцем ефективності операцій, що максимізує сили й концентрує можливості ураження інших існуючих засобів”, і там же “ISTAR буде центром домінування на полі бою і в передбачуваному майбутньому” [1, 2].

За два роки до початку військової агресії на Україну система ISTAR була детально розібрана в серії статей українських авторів [3-5], де було наголошено на критичній необхідності її імплементації в управлінні військами України [6,7].

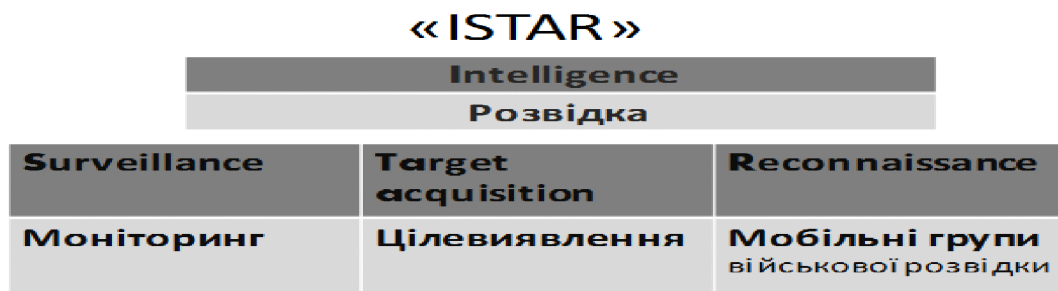
Мережоцентрична концепція та її складові постійно оновлюються, їх розбори наводяться в об’єднаних доктринах НАТО [8-14], а також у публікаціях країн, які нещодавно стали членами НАТО [15-20].

Метою статті є показ на існуючих прикладах реальності підвищення бойової ефективності підрозділів за допомогою систем, що зменшують довжину ланок “бойовий простір – командир” і “командир – бойовий простір”, наголошення на необхідності узагальнення позитивного бойового досвіду, набутого підрозділами в бойових діях на тактичному і оперативному рівнях в організації горизонтальних зв’язків, уніфікації процедур і оновлення підходів до управління військами України.

**Виклад основного матеріалу.** Розвиток засобів телекомунікації в кінці XX ст. призвів до настання інформаційної ери у веденні бойових дій. “Протягом історії ведення бойових дій пристосовувалось до характеристик свого часу і технологій свого часу. Сьогодні ми бачимо тенденції переходу від індустріальної ери ведення бойових дій з її акцентами на накопиченні маси до інформаційної ери з виділенням необхідності поєднання всіх сил в одну мережу і поширення ситуаційної обізнаності. У контексті цього переходу мережецентрична війна (МЦВ), або Network-centric warfare (NCW), є однією з ключових

концепцій у розумінні характеру операцій в майбутньому” [14]. Поєднуючи всі бойові одиниці в одну мережу концепція МЦВ фокусується на збільшенні ефективності бойової міці існуючих елементів за рахунок завоювання інформаційної переваги і концентрації необхідної кількості сил у потрібному місці на визначений час.

Концепція МЦВ реалізується в системі ISTAR, яка є сферою застосування розвідки, де інтегруються процеси розвідки, спостереження та визначення цілей для покращення ситуаційної обізнаності командирів, їх спроможності правильно та своєчасно розуміти зміст, сенс, значення, обставини та умови будь-якої зміни оперативної (бойової) обстановки, приймати обґрунтовані (доцільні) рішення. Система ISTAR включає взаємопроникаючі організаційну і технічну системи та є добре організованим, чітко скоординованим, об’єднаним застосуванням сил і засобів розвідки згідно з установленими протоколами і процедурами [7]. Структурно в системі ISTAR об’єднані чотири первинні модулі: розвідка, моніторинг, цілевиявлення, мобільні групи військової розвідки (рис. 1).

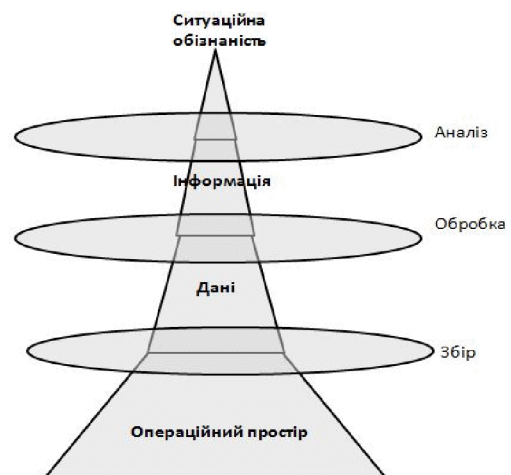


**Рис. 1. Модульна структура системи ISTAR**

Таке структурування засобів розвідки сприяє безперервному функціонуванню циклу розвідки: “Управління збором даних” – “Збір” – “Обробка” – “Аналіз” – “Поширення” [11] і призначене для виробництва ситуаційної обізнаності із зібраних даних і наявної інформації шляхом обробки, аналізу і поширення. Співвідношення між даними, інформацією та ситуаційною обізнаністю наведено на рис. 2. Ситуаційна обізнаність відрізняється від інформації тим, що дає змогу розуміти і передбачати майбутні ситуації. Саме вона необхідна в процесі прийняття рішення для виконання місії за наявних обставин METT-TC (Mission - Місія, Enemy - Противник, Terrain - Місцевість, Troops - Власні сили, Time - час, Civil Considerations - Цивільний аспект) [10].

У структурі ISTAR модулі “моніторинг”, “цілевиявлення” та “військова розвідка” (STAR) виконують процеси циклу розвідки зі збору та обробки, а модуль “розвідка” (I) – з аналізу, поширення та управління.

Кроки системи ISTAR [21] повністю відповідають класичному циклу розвідки, але містять у собі процеси безперервної взаємointegraції модулів системи за рахунок циркуляції інформації горизонтально на кожному кроці (рис. 3).

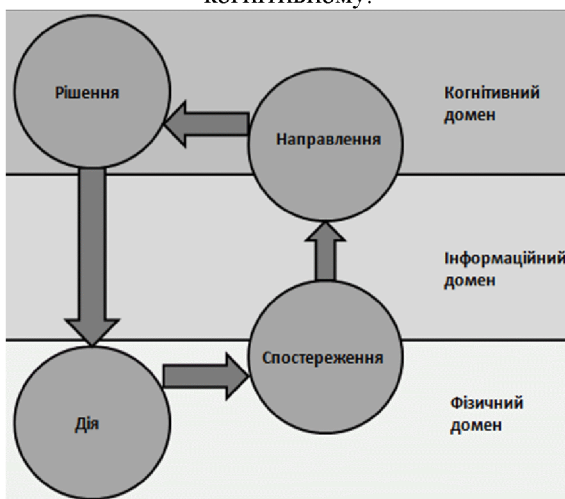


**Рис. 2. Співвідношення між даними, інформацією та ситуаційною обізнаністю**



**Рис. 3. Кроки ISTAR**

Сама система в цілому інтегрується в цикл прийняття рішення “Спостереження” – “Направлення” – “Рішення” – “Дія” (СНРД) (рис. 4) і виконує процеси циклу спостереження і направлення. Управління військами, як і будь-яка система управління, функціонує в трьох доменах: фізичному, інформаційному, когнітивному.



**Рис. 4. Цикл прийняття рішення**

*Фізичний домен* – місце, де відбуваються події, залучаються сенсори і діють бойові підрозділи. Дані, що з’являються в фізичному домені передаються в інформаційний домен.

В *інформаційному домені* виробляється, обробляється і поширюється інформація, на цьому рівні передається командування і контроль військами, а також отримується намір командира з когнітивного домену.

У *когнітивному домені* виникають обізнаність, розуміння, передбачення і, як результат, приймається рішення. Саме в цьому домені багато битв і війн були насправді виграні або програні [14].

*Досвід побудови системи ISTAR в АТО.* У 2017 р. в одній зі смуг проведення АТО в період масованого застосування противником артилерії

було вирішено залучити систему контрбатареїної боротьби. За рівних початкових можливостей в аспектах фортифікації, якості озброєння і технічного оснащення результат протягом останнього часу був на користь тих сил, які були більш організовані в мережі управління. У разі, коли можливості управління обох сторін рівні, протистояння зміщується в інші площини [14]. Побудову системи контрбатареїної боротьби було здійснено за принципами системи ISTAR (рис. 5).

1. *Організація збору даних* була представлена структурою трьох модулів S-TA-R у фізичному домені:

- у модулі моніторингу було задіяно принцип “глибокого сенсорного застосування” – усі доступні сенсори 24 години на добу були зав’язані до єдиної інформаційної мережі: стаціонарні пости передового спостереження (FO), електронно-оптичної (EO MASINT), комунікаційної (COMINT), електронно-сигнальної (ELINT) розвідок. “ISTAR – це заняття для всіх, пара очей це засіб ISTAR” [21].

- у модулі цілевиявлення були задіяні засоби інструментальної розвідки (MASINT).

- у модулі військової розвідки були задіяні групи артилерійських коригувальників з секціями БПЛА.

Розвиток комунікацій дав змогу обладнати кожний пост і кожну групу засобами моніторингу і комунікації, що зробило можливим передачу даних у реальному часі з фізичного в інформаційний домен з кожного з численних постів у смузі моніторингу.

2. *ISTAR* – це система систем. Вона складається з окремих систем, підрозділів, штабів, і вони стають більш ефективними шляхом взаємодії та координації їх дій [18]. При виконанні циклу розвідки “обробка” модулі S-TA-R були посилені штабами, які дані з фізичного рівня перетворювали на інформацію, поширювали її з метою співставлення даних, отриманих іншими модулями з фізичного домену. У визначенні системи ISTAR ключовим є взаємопроникнення систем. Одні й ті самі події та факти одночасно фіксуються декількома учасниками системи різними засобами. Коли учасники не тільки фіксують ту саму подію, але також мають можливість обговорити її або використати у взаємодії (рис. 6), така інформація може бути поширена і якісно збагачена [22]. Таке якісне збагачення відбувається при обробці інформації в контексті інших пов’язаних даних. Цінність такої взаємодії полягає в можливості на вищих рівнях досягти знання і розуміння, а, як наслідок збільшення ефективності дій.



Рис. 5. Принципова схема функціонування ISTAR у розвідувально-вогневому комплексі (РВК)

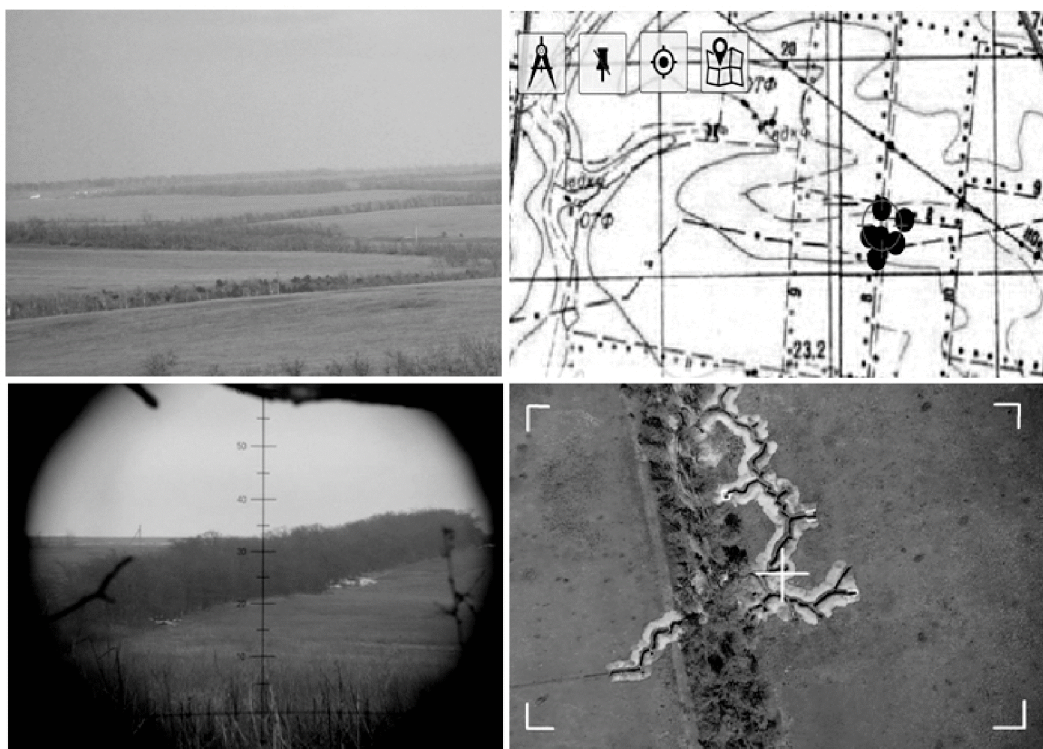


Рис. 6. Співставлення пов'язаних даних з різних модулів STAR

Для виміру якості інформації вона має відповідати одночасно 5 критичним вимогам: повнота, достовірність (порівняння з пов'язаними джерелами), поточність (у реальному часі), точність, доступність. Усі ці критерії є незалежними. Інформація може бути повною, але недостовірною, точною та достовірною, але несвоєчасною тощо [22, 23]. Незначні дані набувають важливості в поєднанні з одночасними даними з інших сенсорів, інші дані виявляються помилковими і непідтвердженими пов'язаними джерелами. Взаємодія модулів STAR у фізичному та інформаційному доменах шляхом циркуляції

інформації (\* на рис. 5) забезпечує відсортування адекватних даних від таких, що не відповідають вимогам, дає можливість у реальному часі відкоригувати процес збору даних і після обробки даних поширити якісно збагачену інформацію для аналізу на наступний модуль – І.

3. Наступний крок ISTAR – “аналіз” якісно збагаченої інформації здійснювався в центрі управління артилерією (Fire direct center-FDC) [11]. Оперуючи у взаємопроникаючому інформаційному середовищі при аналізі інформації були застосовані нові технології візуалізації бойового простору, які допомагали отримати сплав (fusion) наявних даних та

інформації для розвитку ситуаційної обізнаності [8], розуміння і передбачення [26]. Вивчення шаблонів поведінки противника і наявність прямого зв'язку із сенсорами в фізичному рівні давали можливість отримувати інформацію про активність противника майже одночасно з її початком, а часто навіть заздалегідь до її початку на основі передбачення шаблонних дій.

4. *Поширення ситуаційної обізнаності* (\*\* на рис. 5.) відбувалося горизонтально в об'єднаній мережі для підвищення швидкості реагування й можливості коригування управління збором даних сенсорів, приведення до бою підрозділів вогневого ураження в фізичному домені, а також вертикально на ланку управління в когнітивному домені для процесу командирського прийняття рішення. Звичайно, при поширенні ситуаційної обізнаності дотримувались вимог до захищеності інформації: приватність, доступність, вбудованість, автентичність, неможливість відмови від авторства зафіксованих даних [22]. Ситуаційна обізнаність є кінцевим продуктом системи ISTAR, відповідає всім вимогам до інформації та є ненадмірною для полегшення прийняття рішення.

Вхідними даними в систему від командування надходили вимоги до інформації (CCIR – критичні вимоги командира до інформації), розвідки (PIR – першочергові вимоги до розвідки) [20] та “управління збором даних”. Крім того, коригування управління збором даних відбувалось постійно на основі поширеної інформації на нижчих ланках взаємодії всіх елементів модулів.

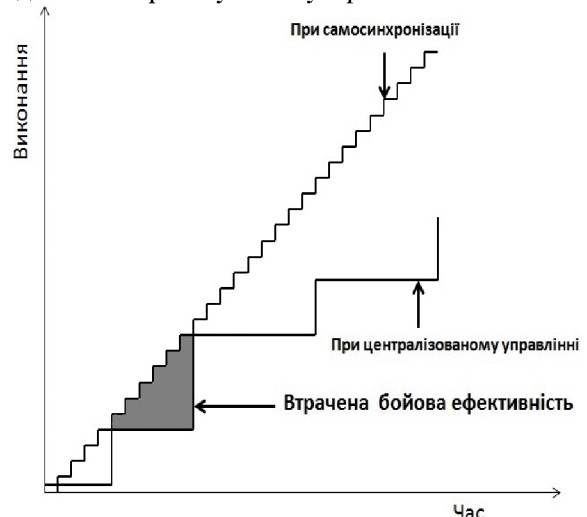
Застосування описаних принципів глибокого сенсорного залучення, поширення інформації та збагачення її якості, донесення ситуаційної обізнаності до всіх авторизованих учасників єдиної мережі призвело до отримання інформаційної переваги над противником: командування в on-line режимі отримувало дані про підготовку або початок активності визначеної артилерійської системи противника з її локалізацією і навіть зображенням з засобів БПЛА або електронно-оптичної розвідки, що полегшувало і пришвидшувало процес прийняття командирського рішення.

*Особливості впровадження системи ISTAR в АТО.* Втілення інформаційної переваги в бойову ефективність виявилось неможливим без впровадження принципів мережоцентричності до всієї системи РВК. Слабкість однієї ланки ослаблює ланцюг в цілому [2]. Незважаючи на якісний продукт системи ISTAR, вогневі підрозділи у фізичному домені продовжили управлятися у вертикальній ієрархії: на рис. 5. чорними стрілками показаний потік інформації в циклі прийняття рішення при централізованому управлінні військами. Занадто великий час

проходження даних з фізичного домену через інформаційний і когнітивний знов у фізичний і недолучення бойового підрозділу до мережі управління спричинило як запізнілий початок дій, так і неефективність дій через неможливість реагування на поточні зміни в бойовому просторі без зв'язку з когнітивним доменом довгим рядом ланок управління.

Для досягнення підвищення бойової ефективності вогневих підрозділів було обґрунтовано доцільність долучення останніх до мережі ISTAR. З отриманням доступу до загальної оперативної картини, поширеної ситуаційної обізнаності (\*\* на рис. 5), даних у реальному часі в фізичному домені (\*\*\*) на рис. 5) вогневі підрозділи отримали здатність самосинхронізації бойових дій. Самосинхронізація (self-synchronization) відбувається у фізичному домені при спусканні ініціативи на нижчий рівень, послабленні традиційного ієрархічного підходу до командування [24], долученні всіх авторизованих учасників системи РВК до ситуаційної обізнаності on-line і призводить до більш швидкого і ефективного виконання бойової задачі завдяки дробленню циклів прийняття рішення СНРД [25] і можливості швидко вносити корективи на внутрішні зміни системи і зовнішні чинники бойового простору (рис. 7.).

Завдяки залученню до мережі всіх учасників РВК система ISTAR поширювала ситуаційну обізнаність, сенсори і вогневі підрозділи мали можливість пристосовувати свої дії до ситуації на тактичному рівні, командир мав усі засоби для швидкого прийняття доцільного рішення і поширення його до виконання – усе це дало змогу відновити втрачену бойову ефективність.



**Рис. 7. Втрата бойової ефективності при централізованому управлінні військами**

Алгоритм дій відповідав схемі на рис. 5:

- пости моніторингу сповіщали про підготовку або початок активності артилерійських систем противника;

- групи військової розвідки і БПЛА починали точкове спостереження вузької локації бойового простору, одночасно вогневі підрозділи приводились до бою, маючи розуміння і обізнаність про ситуацію, одночасно командир мав приймати рішення;

- сенсори інструментальної розвідки або групи військової розвідки підтверджували дані постів моніторингу;

- у лічені секунди ситуаційна обізнаність поширювалась у вигляді координат (X, Y) і зображення;

- на час прийняття командиром рішення і поширення наміру командира у фізичний домен всі підрозділи фізичного домену вже володіли ситуаційною обізнаністю, були готові виконувати місію та самостійно реагувати на зміни бойового простору в межах наміру командира. Швидкість командування забезпечувалась вичерпністю ситуаційної обізнаності, що робило можливим прийняття рішення за секунди і поширення наміру командира різними засобами комунікації від голосової команди “Уразити” до тактичного символу відповідному абоненту в системі управління боєм;

- групи і пости модулів STAR підтверджували виконання місії або запускали нові ітерації циклів розвідки і прийняття рішень СНРД;

- після виконання місії фото- та відеоматеріали, дані сенсорів (рис. 6) накопичувались в модулі І, аналізувались і поширювались для внесення коректур на основі обов’язкового післяопераційного розбору (after action review).

Таким чином, при залученні системи контрбатареїної боротьби, побудованої за принципами ISTAR впродовж трьох місяців (рис. 8) кількість ураження активних артилерійських систем противника в окремій смузі відповідальності зросла в 10 разів: з X одиниць на місяць до 10X (рис. 9). Показово, що зростання ефективності бойового застосування вогневих підрозділів відбулося тільки після

впровадження принципів мережоцентричності всіма учасниками РВК (рис. 10).

Після понесення значних втрат у вогневій міці противник програв ініціативу і значно зменшив застосування артилерійських систем. Визнаючи роль самосинхронізації в підвищенні ефективності вогневих підрозділів командування, втім, хибно приписало це ініціативі на нижчому рівні, тому систему контрбатареїної боротьби було знято, лишилися тільки сенсори та вогневі підрозділи у фізичному домені та прямий зв’язок між ними. Відсутність системи систем викликало іншу перепону для підтримання бойової ефективності на належному рівні: гігабайти даних з фізичного рівня сповільнили швидкість командування, не відбувалось збагачення якості інформації шляхом її взаємопроникаючого поширення (\* на рис. 5), зникли підстави для розуміння і передбачення, через відсутність ситуаційної обізнаності сенсори і вогневі підрозділи втратили здатність самосинхронізації і ефективність знову знизилася до попередніх показників (рис. 9). Слабкість однієї ланки послабила весь ланцюг.

Кореляція між залученням системи ISTAR у РВК з принципами мережоцентричного управління та зростанням бойової ефективності вогневих підрозділів артилерії (рис. 11) наочно демонструє необхідність і можливість переходу до новітніх методів управління військами.

**Висновки.** Концепція мережоцентричних операцій застосовує інформаційні технології для можливості з’єднання в мережі ланок “сенсор – система ураження” (sensor-to-shooter) напряму, з одночасним зменшенням проміжку часу прийняття командирських рішень та їх поширення ланкою “командир – система ураження”. Досягнення скорочення в часі виконання циклу “першим побачив – першим зрозумів – першим почав дію – першим виконав місію” ( see first, understand first, act first, and finish decisively) [9] лише на декілька відсотків призводить до завершення місії раніше за противника і дає досягти переваги на полі бою над ворогом рівним та навіть таким, що має перевагу в кількісному складі.

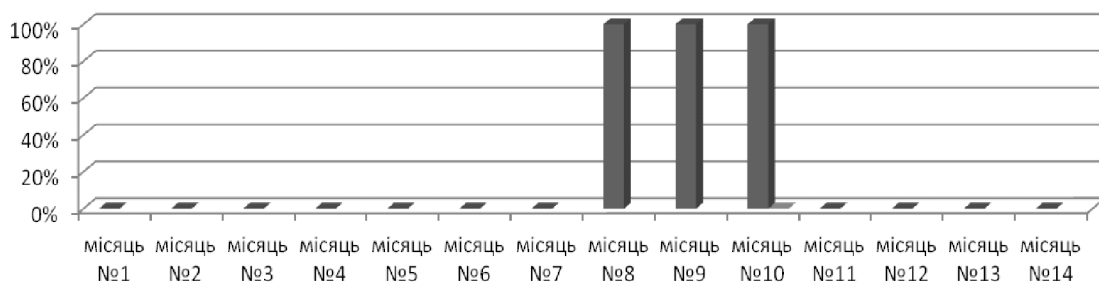
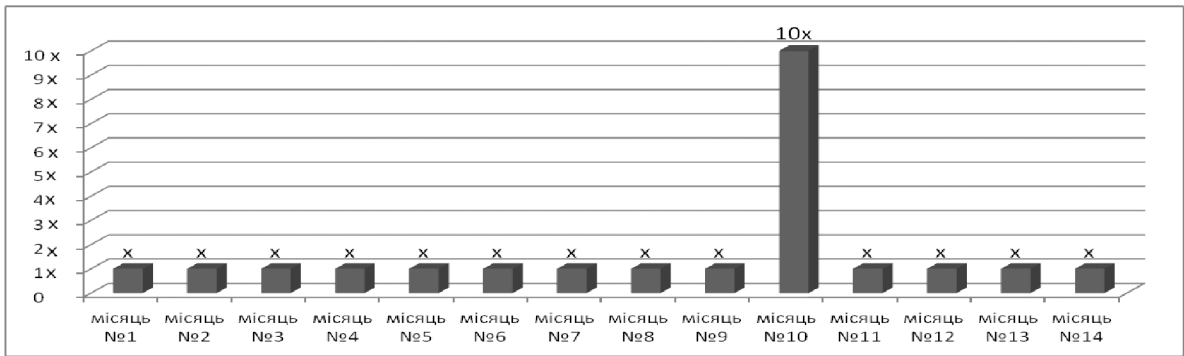
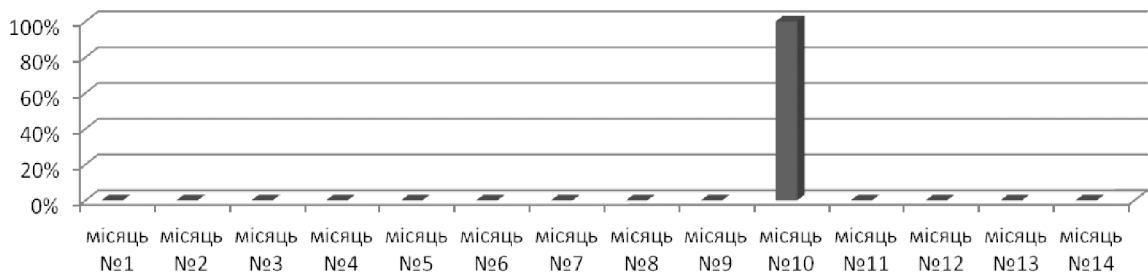


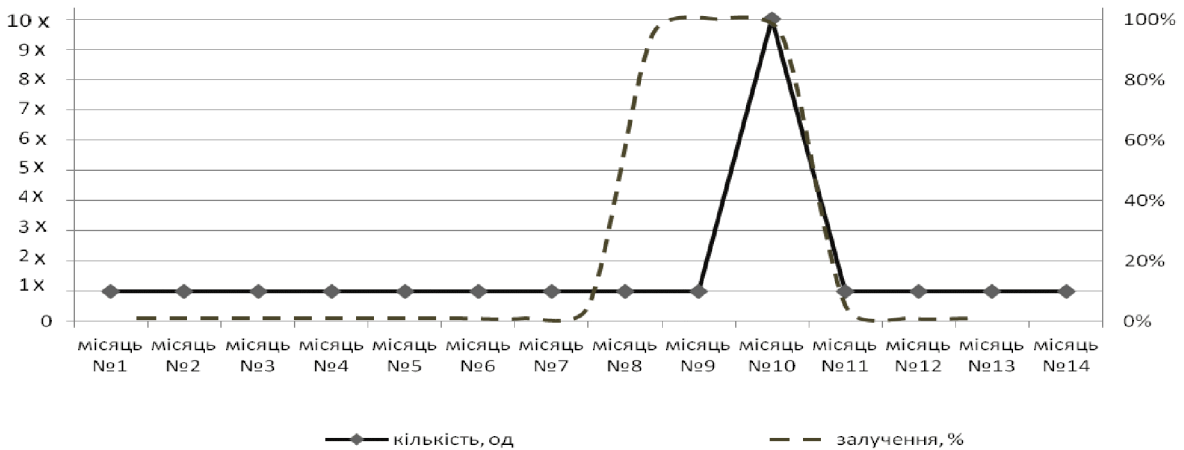
Рис. 8. Залучення системи контрбатареїної боротьби, побудованої за принципами ISTAR



**Рис. 9. Кількість уражених активних артилерійських систем противника**



**Рис. 10. Залучення вогневих підрозділів РВК за принципами мережоцентричності**



**Рис. 11. Кореляція між залученням системи ISTAR у РВК з принципами мережоцентричного управління та зростанням бойової ефективності вогневих підрозділів артилерії**

Застосування системи ISTAR дає змогу скоротити час від спостереження до ураження з десятків хвилин до лічених секунд. Цього можна досягти лише злагодженою роботою структурних взаємодіючих елементів системи і впровадженням заходів, які дають змогу подолати перепони у зборі, обробці та розповсюдженні інформації. Важливий кожний крок ISTAR:

- глибоке сенсорне застосування при зборі та спостереженні;
- поширення інформації в мережі при обробці для якісного її збагачення;
- поширення ситуаційної обізнаності до всіх авторизованих елементів системи;

- скорочення часу прийняття командирського рішення з одночасним долученням системи ураження до інформаційної мережі та наділенням її ініціативою коригування дій при виконанні місії в рамках наміру командира залежно від зміни ситуації в бойовому просторі.

Для забезпечення спроможності виконання кожного з цих кроків у всіх смугах військового протистояння вимагається запровадження програм на державному рівні. І це світова практика нині навіть у країнах-членах НАТО: “Ми відмітили, що Міністерство оборони сконцентрувало головні зусилля на покращенні процесу збору. Однак значні покращення все ще

потрібні у процесах обробки та поширення зібраної інформації”, “Можливості Збройних Сил обробляти та поширювати зібрану інформацію значно відстають від можливостей засобів збору. Ми рекомендуємо Міністерству оборони визнати проблему” [2].

Досвід застосування в сучасному збройному конфлікті системи ISTAR інтегрованої до РВК, довів, що один вогневий підрозділ може стати більш результативним за всі інші підрозділи в смузі відповідальності та, що більш показово, ефективнішим за самого себе до долучення до системи ISTAR. Вивчення досвіду власних підрозділів є вкрай важливим для уніфікації процедур організації розвідки в єдиний стандарт, а імплементація новітніх підходів до управління військами є нагальною необхідністю для підвищення ефективності застосування українських бойових підрозділів під час відбиття військової агресії противника, що переважає в накопиченій міці.

#### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. House of Commons. Session 2007-08. The contribution of Unmanned Aerial Vehicles to ISTAR capability. Publications on the internet. Defence Committee Publications. Defence – Thirteenth Report [Електронний ресурс]. – Режим доступу: <https://publications.parliament.uk/pa/cm200708/cmsselect/cmdfence/535/535.pdf>.
2. House of Commons. Session 2009–10. The contribution of ISTAR to operations. Publications on the internet. Defence Committee Publications. Defence – Eighth Report [Електронний ресурс]. – Режим доступу: <https://publications.parliament.uk/pa/cm200910/cmsselect/cmdfence/225/225.pdf>.
3. Пашук Ю. Місце і роль ISTAR у системах розвідки провідних країн світу / Ю. М. Пашук, Ю. П. Сальник // Військово-технічний збірник. – 2012. – №2(7). – С. 94-102.
4. Пашук Ю. Система ISTAR – критичний елемент досягнення інформаційної переваги у сучасних війнах та конфліктах. / Ю. М. Пашук, Ю. П. Сальник // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2012. – №3(32). – С. 21-30.
5. Пашук Ю. Роль об'єднаної системи ISTAR НАТО при проведенні широкого спектра військових операцій / Пашук Ю.М., Алексєєв В.М., Сальник Ю.П. // Інтелектуальна оборона: Збірка праць «IV Січевих ГІСів» (науково-практичний форум / Академія сухопутних військ імені гетьмана Петра Сагайдачного: Львів, 22–24 січ. 2013 р.). – Львів: АСВ, 2013. – С.28-30.
6. Pashchuk Y. Implementation of ISTAR in Ukrainian Forces / Y.Pashchuk,Y.Salnyk // Військово-технічний збірник. – 2013. – №1(8). – С. 64-71.
7. Сальник Ю. Шляхи впровадження концепції ISTAR у систему розвідки Збройних Сил України / Ю. П. Сальник, Ю. М. Пашук // Системи озброєння і військова техніка. 2014. – №1(37). – С. 72-75.
8. B-GL-352-001/FP-001. Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR). Ottawa: National Defence and the Canadian Forces. – 2004. – 113p.
9. U.S. Army Field Manual (FM) 6-0: Command and Control of Army Forces. – Department of the Army. – Washington,DC, 11 August 2003 [Електронний ресурс]. – Режим доступу: [http://www.bits.de/NRANEU/others/amd-usarchive/fm6\(03\).pdf](http://www.bits.de/NRANEU/others/amd-usarchive/fm6(03).pdf).
10. U.S. Army Field Manual (FM) 3-0: Operations Department of the Army Washington, DC, 22 February 2011. [Електронний ресурс]. – Режим доступу: <https://fas.org/irp/doddir/army/fm3-0.pdf>.
11. JP 2-0: Joint Intelligence. 22 October 2013 [Електронний ресурс]. – Режим доступу: [http://www.dtic.mil/doctrine/new\\_pubs/jp2\\_0.pdf](http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf).
12. JP 3-09: Joint fire support. 14 December 2014 [Електронний ресурс]. – Режим доступу: [http://www.dtic.mil/doctrine/new\\_pubs/jp3\\_09.pdf](http://www.dtic.mil/doctrine/new_pubs/jp3_09.pdf).
13. JP 3-55: Doctrine for Reconnaissance, Surveillance, and Target Acquisition Support for Joint Operations (RSTA). 14 April 1993 [Електронний ресурс]. – Режим доступу: [http://www.bits.de/NRANEU/others/jp-doctrine/jp3\\_55\(93\).pdf](http://www.bits.de/NRANEU/others/jp-doctrine/jp3_55(93).pdf).
14. The implementation of network-centric warfare. Washington. D.C. Office of the Secretary of Defense, 2005 [Електронний ресурс]. – Режим доступу: <http://handle.dtic.mil/100.2/ADA446831>.
15. Psik. ISTAR system building in the army of the Czech Republic. / Psik, Cech // Economics and Management, Brno: University of Defence, 2012 [Електронний ресурс]. – Режим доступу: [https://www.unob.cz/eam/Documents/Archiv/EaM\\_1\\_2012/PSIK\\_CECH.pdf](https://www.unob.cz/eam/Documents/Archiv/EaM_1_2012/PSIK_CECH.pdf).
16. Psik. Perspektiva systému ISTAR/ISR. /Psik, Cech // Economics and Management, Brno: University of Defence, 2012 [Електронний ресурс]. – Режим доступу: [https://www.unob.cz/eam/Documents/Archiv/EaM\\_2\\_2012/Psik\\_Cech.pdf](https://www.unob.cz/eam/Documents/Archiv/EaM_2_2012/Psik_Cech.pdf).
17. Podhorec. Perspectives of ISR System and Its Role in Task Forces. /Podhorec, Tuček, Samárek // Economics and Management, Brno: University of Defence, 2012. [Електронний ресурс]. – Режим доступу: [https://www.unob.cz/eam/Documents/Archiv/EaM\\_2\\_2012/Podhorec\\_Tuček\\_Samárek.pdf](https://www.unob.cz/eam/Documents/Archiv/EaM_2_2012/Podhorec_Tuček_Samárek.pdf).
18. The Dutch Approach of ISTAR Concept during NRF-4 // Doctrine. – 2006. #9. – p. 65-69. [Електронний ресурс]. – Режим доступу: [http://www.cdef.terre.defense.gouv.fr/publications/doctrine/doctrine09/version\\_us/foreign\\_studies/art04.pdf](http://www.cdef.terre.defense.gouv.fr/publications/doctrine/doctrine09/version_us/foreign_studies/art04.pdf).
19. The ISTAR Capability of the Canadian Forces. // Doctrine. – 2006 #9. - p. 63-64 [Електронний ресурс]. – Режим доступу: [http://www.cdef.terre.defense.gouv.fr/publications/doctrine/doctrine09/version\\_us/foreign\\_studies/art04.pdf](http://www.cdef.terre.defense.gouv.fr/publications/doctrine/doctrine09/version_us/foreign_studies/art04.pdf).



20. Intelligence Collation in Asymmetric Conflict: A Canadian Armed Forces Perspective by G.Thibault. - 2007 10th International Conference on Information Fusion. [Электронный ресурс]. – Режим доступа: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.689.1563&rep=rep1&type=pdf>.
21. Field Army ISTAR Handbook. 14 June 2007 [Электронный ресурс]. – Режим доступа: <http://www.operationtelic.co.uk/documents/uk-istar-handbook-2007.pdf>.
22. Understanding Information Age Warfare, by Alberts, Garstka, Hayes, and Signori. – CCRP Press, 2001. [Электрон. ресурс]. – Режим доступа: [http://www.au.af.mil/au/awc/awcgate/ccrp/alberts\\_uiaw.pdf](http://www.au.af.mil/au/awc/awcgate/ccrp/alberts_uiaw.pdf).
23. Network centric warfare : developing and leveraging information superiority, by Alberts, Gratska, Stein – 2000. [Электрон. ресурс]. – Режим доступа: [http://www.dodccrp.org/files/Alberts\\_NCW.pdf](http://www.dodccrp.org/files/Alberts_NCW.pdf).
24. Enablers of Self-Synchronization for Network-Centric Operations: Design of a Complex Command and Control Experiment by Hutchins, Kleinman, Hoesavar, Kemple, Porter Proceedings of the 6 the international command and control research and technology symposium, CCRP, Annapolis, MD, USA, 2001. [Электронный ресурс]. – Режим доступа: <http://www.dtic.mil/dtic/tr/fulltext/u2/a468216.pdf>.
25. Smith E. Jr. Network-centric warfare. What's the Point? // US Naval War College Review, 2001. [Электронный ресурс]. – Режим доступа: <https://usnwc2.usnwc.edu/getattachment/c2438fba-7ada-41cb-bf9e-85cfff4dc258/Network-centric-Warfare--What-s-the-Point-.aspx>.
26. A Network-Centric Operations Case Study: US/UK Coalition Combat Operations During Operation Iraqi Freedom. – Department of Defence. – 2 March 2005 [Электронный ресурс]. – Режим доступа: <http://www.dtic.mil/get-tr-doc/pdf?AD=ADA457357>.

Стаття надійшла до редакції 27.10.2017

### **Прозапас И. Н.**

В/ч 3057, Мариуполь

#### **Опыт построения системы ISTAR в АТО, особенности внедрения и препятствия на пути повышения боевой эффективности огневых подразделений**

**Резюме.** В статье приведен пример построения и интеграции системы ISTAR в сетевую модель управления подразделениями в современном военном конфликте. Этот опыт является актуальным в контексте неизбежного изменения подхода к управлению войсками и необходимости повышения боевой эффективности подразделений Украины в противостоянии военной агрессии.

**Ключевые слова:** цикл разведки, цикл принятия решения, сенсоры, сеть, распространенная информация, ситуационная осведомленность, требования к информации, намерение командира, самосинхронизация.

### **I. Prozapas**

М/ч 3057, Mariupol

#### **An experience of construction of ISTAR in ATO, peculiarities of its implementation and impediments on the way to increasing the combat efficiency of forces**

**Resume.** The article gives an example of the construction and integration of the ISTAR system in the network centric model of forces command and control in the modern military conflict. The achieved result due to the implementation of the system ISTAR shows the possibility of improving the efficiency of military units by means of applying of standard procedures developed in the armies of the leading countries of the world. This example is urgent in the context of the inevitable changes in the approach to the command and control and the necessity of increasing the combat efficiency of Ukrainian units in the current military aggression.

**Keywords:** intelligence cycle, decision making cycle, sensors, network, shared information, situational awareness, information requirements, commander's intent, Self-Synchronization.