

УДК 001.4:002.6+340.68:355.01

**ТОМЧЕНКО О.В.**, Науковий центр аерокосмічних досліджень Землі  
Інституту геологічних наук Національної академії наук України  
**ЧЕРНЕНКО О.Є.**, Всеукраїнський благодійний Фонд сприяння розвитку  
геоінформаційних технологій та послуг “ГІС-Асоціація України”

## ДО ПИТАННЯ ВИЗНАЧЕННЯ ПОНЯТІЙНОГО АПАРАТУ СУЧАСНИХ “ІНФОРМАЦІЙНИХ ВІЙН”

***Анотація.** Про понятійний апарат сфери “інформаційних війн”, критерії і методи ідентифікації, а також відповідності їх змісту певній якості.*

***Ключові слова:** інформаційна війна, інформаційна безпека, правопорушення в інформаційній сфері, математичне моделювання, сучасні інформаційні технології, методи та засоби управління.*

***Аннотация.** О понятийном аппарате сферы “информационных войн”, критериях и методах идентификации, а также соответствия их содержания определенному качеству.*

***Ключевые слова:** информационная война, информационная безопасность, правонарушение в информационной сфере, математическое моделирование, современные информационные технологии, методы и средства управления.*

***Summary.** About the conceptual framework of sphere of “informative wars”, criteria and methods of authentication, and also accordance of their nature to certain quality.*

***Keywords:** information war, information safety, offence in an information sphere, mathematical design, modern information technologies, methods and management facilities.*

**Постановка проблеми.** Дослідження правопорушень в інформаційній сфері знаходиться в площині інформатики, юриспруденції, політології, психології, системного аналізу, соціально-економічних і культурно-історичних процесів та певного ряду суміжних дисциплін. Тобто, воно має міждисциплінарний характер.

З огляду на інформаційний характер суспільства, суцільну інформатизацію процесів, які в ньому відбуваються, вважаємо доцільним звернути увагу на дві взаємопов’язані обставини, які остаточно сформувались у ХХІ столітті.

**Перша обставина.** Правопорушення в інформаційній сфері досить часто неможливо виявити (те, що мав місце факт правопорушення, ми часто розуміємо тоді, коли маємо справу з його наслідками), в разі виявлення ознак правопорушення в інформаційній сфері ми здебільшого потрапляємо в ситуацію, коли відсутні надійні ідентифікатори та методи, які дозволяють однозначно кваліфікувати ці правопорушення по суті. І нарешті – в тих випадках, коли правопорушення в інформаційній сфері кваліфіковано по суті, вжиття заходів з організації протидії та притягнення винних до відповідальності ускладнюється відсутністю відповідної юридичної бази та недосконалістю понятійного апарату.

**Друга обставина.** Понятійний апарат та юридична база, які використовуються сьогодні, успадковані нами з другої половини минулого ХХ сторіччя. З огляду на характер процесів, які відбуваються сьогодні у Світі, ми маємо зрозуміти – змінився не просто характер протистояння, змінилась сама його суть. Така зміна, відповідно, вимагає формування нового понятійного апарату та суттєвої корекції юридичної бази саме по суті.

**Метою статті** є висвітлення питань, пов’язаних з формуванням понятійного апарату “інформаційних війн”, який потребує дослідження та визначення в нових умовах, що фактично існують сьогодні. А саме, розкрити критерії та методи ідентифікації відповідності змісту термінів понятійного апарату певній якості фактологічного наповнення.

**Виклад основних положень.** Сьогодні світ переходить до якісно нового стану – інформаційного суспільства, тобто до такої форми і способу організації дійсності, за якої інформаційна сфера стає пріоритетною областю людської діяльності. Керівники провідних країн світу у 2000 р. зафіксували в “Окінавській Хартії глобального інформаційного суспільства” (Окінава, 22 липня 2000 р.) один з головних критеріїв нового стану цивілізації – вплив інформаційно-комунікаційних технологій на формування суспільства двадцять першого століття [1].

Експерти в галузі інформації відзначають, що “інформаційне суспільство” не має політичних, соціальних та економічних кордонів [2].

У силу цього в юриспруденції останніх десятиліть ХХ століття з’явилися нові, які ще перебувають в процесі розробки, концепції інформаційного права і права інформаційних технологій. У відповідності з поняттями сучасної кібернетики та інформатики, інформаційне право в даний час визнає інформацію в якості третього фундаментального чинника буття на рівні матерії та енергії. Ця концепція будується на основі емпіричного аналізу. Вона розглядає інформацію та інформаційну сферу (кібернетичний простір) як новий економічний, культурний і політичний капітал [3].

Одночасно з появою нового інструментарію, зміною самого простору безпеки, змінюються завдання і цілі, і все це певним чином є взаємозалежним.

На думку заступника міністра оборони США П. Вулфовіца: “Ми рухаємося від межі, яка фокусувалась у минулому на відомих погрозах до більш гнучкої межі, заснованої на можливостях захищати себе від мінливих і невідомих погроз... від фокусу на програмах і платформах до фокусу на результатах... від сегментованої інформації і закритої інформаційної архітектури до мережевої інформації і відкритої архітектури...” [4]. Він веде мову про принципову зміну всієї парадигми війни.

Дж. Арквілла і Д. Ронфельдт дослідили концепцію “Сетєцентричної (мережевої) війни”. Вони підкреслили, що вона не закінчується тільки Інтернетом [5]. Інформаційна революція підсилила мережеву форму організації, чим скористалися у воєнних цілях. Інформаційна революція також створила залежність бойових дій від інформації та комунікації. Зростаюча роль недержавних гравців і мережеві форми організації з’єдналися, щоб відтворити можливість сумновідомих подій 11 вересня 2001 р. Дослідники вбачають необхідність, в майбутньому, захист ціннісної системи суспільства, оскільки інформація не тільки важлива як процес, а і виконує структурну роль, що програмує організацію системи [6]. Автори вважають, що в майбутньому інформаційна революція зробить ідеї більш важливими, ніж матеріальні об’єкти. Виходячи з усіх цих причин, інформаційна стратегія стає окремим виміром великої стратегії.

Останній час лунають заклики взагалі відмовитись від терміну “інформаційна війна”. Дозволимо собі з цим не погодитись.

Саме зміна суті процесів в інформаційній сфері, їх ролі в суспільному житті, обумовлюють існування терміну “інформаційна війна” як такого, який відображає стан процесів протиборства в інформаційній сфері у випадках, коли воно носить недоброзичливий характер, порушує усталені юридичні чи морально-етичні норми, як в міждержавних відносинах, так і в інформаційних середовищах суверенних держав.

Однозначне, адекватне суті процесів, розуміння термінів, категорій, структури сучасних “інформаційних війн” – усіх, пов’язаних з цим понять і фактів які мають юридичне значення, надає нам можливості:

- мінімізації ризиків та загроз при середньо- та довготерміновому плануванні;
- адекватного сприйняття викликів для формування симетричної протидії;
- подолання наслідків та збитків, спричинених “інформаційними війнами”;
- формування висновків і корекції планів у відновлювальний період.

Превентивні дії по упередженню зростаючих загроз “інформаційних війн” повинні мати потужний аналітичний, індикативний та практичний механізми. Введення в дію та застосування цих механізмів має бути відпрацьовано, в тому числі – в юридичній площині. Коротко кажучи, вживаючи термін, наприклад: “підбурення до агресії”, “антидержавний виступ” чи “асоціальний прояв” ми маємо чітко уявляти, що саме це означає по суті а також чітко і однозначно кваліфікувати – маємо ми підстави чи ні визначити конкретний факт певним чином.

Що ми маємо на увазі під поняттям “інформаційна війна”?

Термін “війна” – ми розуміємо, як вчинення певних дій, спрямованих на результат, цілеспрямованої, запланованої заздалегідь діяльності певної сторони, який вона має можливість конвертувати в економіку. Цілі “війни” та її результати мають бути прийнятними для її ініціаторів.

Ведучи мову про те, що у XXI сторіччі характер процесів і характер протиборства в інформаційній сфері змінився “по суті”, ми маємо на увазі наступне. У другій половині XX ст. була сформована парадигма розвитку військового протиборства, яка передбачала суцільний перехід до високотехнологічних видів зброї та засобів ведення війни. Ця парадигма виявилась хибною. Практика довела (на прикладі багатьох військових конфліктів кінця XX – початку XXI століть – Югославія), що в сучасному Світі відсутні прийнятні цілі для високотехнологічного способу ведення війни. Тобто – засоби ведення війни дорожчі, ніж цілі враження та результат, який можливо досягти в разі перемоги. Ініціатор війни, переможець, який спирається виключно на високотехнологічні засоби, у підсумку отримує лише збитки. Така перемога фактично дорівнює поразці.

Виникла об’єктивна необхідність створення концепції нового способу ведення війни. Така концепція отримала назву “Сетецентричної війни”. Суть її полягає в тому, що основна роль зі сфери безпосередньо військового протиборства переходить до інформаційного середовища та ЗМІ. З високотехнологічного арсеналу до нової концепції переходять засоби збору та обробки інформації, розвідки, засоби управління, засоби враження, які використовуються “точечно” та наявність ядерного арсеналу, як “стримуєчий фактор”.

Роль інформаційної сфери принципово змінюється відповідно до доктрини нової концепції – ця роль стає провідною для досягнення цілей прийнятними засобами. Зміна військової доктрини полягає у покладанні функцій армійських підрозділів на радикальні угруповання (різного характеру – залежно від обставин). Принципово важливою особливістю такої зміни є можливість взаємодії, при необхідності, радикалів з армійськими підрозділами для досягнення певних цілей, з наступною делегітимізацією радикалів, їх фізичним усуненням та покладанням саме на них усієї повноти відповідальності за ті результати протиборства, які виходять за рамки юридичного поля, грубо порушують усталені морально-етичні норми – формують негативний образ результатів протиборства та їх подальшого використання на користь переможця.

Тобто, суто “військову” частину протиборства (окупація територій, населених пунктів, об’єктів інфраструктури та економічних об’єктів, знищення населення чи

примушення його до втечі) у “сетєцентричних війнах” виконують контингенти нового типу, які мають такі спільні риси – варваризація процесів ведення війни (“сомалізація”), навмисне виведення методів та способів ведення війни за рамки правового поля, за межі існуючих релігійних та морально-етичних норм.

Головна якісна відмінність цих контингентів – їх мінімальна “собівартість”. Підготовка та утримання тисячі одиниць радикального контингенту, озброєного стрілецькою зброєю малої та середньої потужності, в рази дешевша, ніж виробництво та утримання однієї одиниці високотехнологічної зброї (танк, літак, ракетний комплекс). Витрати на відновлення та реабілітацію такого контингенту є символічними, оскільки “людський матеріал, який відпрацював свій ресурс” в разі потреби просто замінюється на інший, який в необмеженій кількості постачають депресивні регіони Світу. Більше того – навколо країни, яка підпадає під ураження, формуються “зони нестабільності”, які виступають надійним джерелом для постачання радикального контингенту в необхідній кількості.

Тобто, в Концепції “Сетєцентричної війни” інформаційна сфера набуває відповідно, нової якості – вона є засобом “прикриття” діяльності таких варваризованих радикальних контингентів, надання їм діям легітимності на потрібний термін. Відповідно, таким чином інформаційна сфера забезпечує легітимність використання результатів, отриманих в ході військового протиборства переможцем.

Тобто ми бачимо, що в понятійному апараті, який був сформований станом на кінець ХХ сторіччя, відсутня взагалі кваліфікація значної частини понять і фактів, які мають юридичне значення, з переліку тих, які сьогодні стали невід’ємною частиною Концепції нового способу ведення війни.

“Інформаційна війна”, поряд з кібервійною, є складовою частиною сучасної “сетєцентричної війни”, має свою власну мету і конкретне завдання і може застосовуватися до початку безпосередньо бойових дій збройних сил, в ході самого збройного конфлікту (коли для досягнення цих цілей залучаються радикальні терористичні чи бандформування, різноманітного характеру), і в наступний за конфліктом період. Якісно проведена інформаційна війна дозволяє уникати “гарячої” фази повномасштабних бойових операцій, обмежити їх локальними конфліктами чи поліцейським реагуванням. Елементами “інформаційних війн” є – інформаційно-психологічні операції (ІПСО).

По суті, “інформаційні війни” (операції) базуються на технологіях комунікативного впливу, які спрямовані на внесення змін у поведінку (цінності, мислення, орієнтацію в суспільстві) індивіда за допомогою модифікації його моделі світу, що здійснюється шляхом внесення змін у інформаційні потоки. Відповідно, головною відмінністю “інформаційної війни” є маніпуляції. З метою підвищення якості таких маніпуляцій, при їх застосуванні використовуються науково обґрунтовані, властиві нам, як соціальним особам, біологічні та психічні особливості, сучасні досягнення наук про людину: закон Вебера-Фехнера, теорія перспектив Данієля Канемана, психофізіологічна закономірність відома як “гаманець Міллера”, техніки НЛП, тощо. Уникнути впливу певних дієвих форм маніпуляцій (наприклад, “розрив шаблону” – техніка НЛП), майже неможливо навіть кваліфікованому фахівцю. Особливо, коли мова йде про кваліфікацію фактів чи подій, які мають юридичне значення.

Відповідно – гостро постає питання чіткого формування сучасного понятійного апарату самого поняття “інформаційна війна”, та адекватної кваліфікації певних засобів та методів її проведення.

Ми можемо виділити декілька спільних відмінностей, характерних для “інформаційних війн” останнього покоління:

*По-перше.* У конфліктах останнього покоління “полем бою” є вся територія зони конфлікту, все суспільство, проти якого супротивник веде війну. Проблема полягає в тому, що сучасні війни, в тому числі – інформаційні, відрізняються від усіх раніше відомих сценаріїв ведення конфліктів подібного роду. Так, одна сторона – класична держава, чи армія, яка підпорядковується нормам міжнародного права, національному законодавству своєї країни та правилам застосування цих норм в ході ведення конфлікту. Друга сторона – це в переважній більшості як громадяни, так і не громадяни цієї держави, не формалізовані радикальні структури, громадянські об’єднання і ЗМІ власної чи інших держав. Досить важко, а інколи – неможливо, юридично визначити певні сторони конфлікту – для подібних випадків застосовується поняття “асиметричної війни”, яке, проте, не має ще чіткого визначення та понятійного апарату.

*По-друге.* Це зниження залежності від централізованих систем, в тому числі – інформаційних. Розосередження поряд зі зростаючим значенням швидкості, вимагає високого ступеня готовності до того, щоб підтримувати ефективність дій за рахунок навколишнього оточення і самого супротивника, залучення ресурсів суспільства, прямої взаємодії з суб’єктами господарювання та громадськістю. Від держав, суспільства, господарюючих суб’єктів це вимагає певного рівня мобілізаційної готовності.

*По-третє.* Ключовою ідеєю стала спрямованість дій на досягнення внутрішнього колапсу сил супротивника, замість його знищення. У число цілей для враження входять такі “речі”, як підтримка цілей ПСГО населенням, релігія, мова та культура супротивника. Величезну важливість має точна ідентифікація стратегічних джерел ворожого бойового потенціалу.

*По-четверте.* Психологічні операції у формі медійно-інформаційного втручання стають фактично переважаючою оперативною і стратегічною зброєю. Протиборчі сторони у “інформаційних війнах” останнього покоління стали настільки майстерними в маніпулюванні ЗМІ з метою зміни громадської думки в країні ураження і в світі, що вмиле застосування ПСГО іноді може зробити зайвим введення в дію бойових підрозділів. Найважливішим об’єктом ураження стає підтримка населенням свого уряду, будь яких дій військового чи гуманітарного характеру, які цей уряд проводить. Телевізійні новини або звернення релігійних лідерів фактично стали більш потужною зброєю оперативного призначення, ніж бронетанкові дивізії.

В цілому уявляється, що в перспективі форми протиборства останнього покоління по всій ймовірності будуть найвищою мірою розосередженими і у більшості не визначеними; межа між миром і війною буде розмита аж до повного зникнення. Війна, в тому числі інформаційна, буде нелінійною в такій мірі, що, цілком можливо, в ній буде ускладнена точна ідентифікація поля бою і лінії фронту чи сторін конфлікту взагалі. Різниця між “громадянським” і “військовим” контингентами ймовірно зникне. Дії будуть одночасно направлені на всю “глибину” території сторін, які беруть участь у протиборстві, включаючи усе їх суспільство, що розуміється не тільки в його фізичному, але і в культурно-історичному та релігійному аспектах. Успіх буде сильно залежати від ефективності спільного управління цивільним і військовим секторами, оскільки лінії розподілу між задачами та відповідальністю військового і цивільного керівництва виявляться розмиті.

Зазначені відмінності ведення “інформаційної війни” та інші об’єктивні умови [7] характеризують параметри сучасного суспільства взагалі та інформаційної сфери

зокрема, як відкриту динамічну нелінійну систему, з властивістю одночасного вирішення багатоцільових задач в реальному часі та просторі.

Звичайно, що в умовах такої “інформаційної війни” доводиться приймати рішення та робити висновки в умовах інтенсивного тиску обставин, невизначеності, дезорієнтації, в умовах, які швидко змінюються непередбаченим чином. Зрозуміло, що в таких умовах чіткий понятійний апарат “інформаційних війн”, адекватні методи протидії та використання однозначних індикаторів виступають єдиним надійним підґрунтям формування юридичної бази для кваліфікації фактів та подій, що мають юридичне значення.

Уникнути маніпулятивного впливу “інформаційної війни” можливо застосовуючи методи, які не підпадають під “вражаючі фактори” ІПСО – маніпуляції, підміну цінностей, рефреймінг змісту чи контексту, “розрив шаблону” тощо [8].

Таким методом є побудова математичної моделі процесів, на базі якої саме, можлива побудова понятійного апарату, точна і однозначна ідентифікація тих самих фактів та подій, які мають юридичне значення.

Математична модель, що застосовується для дослідження та якісного визначення процесу “інформаційної війни”, як ми її розуміємо, це математичні методи, які дозволяють встановити закономірності і оцінити очікувану ефективність процесів, що протікають в соціальній, виробничій, економічній, військовій, політичній сферах, і отримати рекомендації, які мають бути враховані при обґрунтуванні рішення щодо управління цими процесами.

Дослідження “інформаційних війн”, математичне моделювання пов’язаних з ними фактів і процесів, вимагає чіткого розуміння місця і ролі усіх існуючих чинників у загальному процесі управління, який включає вироблення рішення. Вироблення рішення в узагальненому вигляді відбувається за такою схемою: з’ясування завдання (мети дії), оцінка обстановки, формування задуму побудови завдання, вибір математичної моделі і виконання за допомогою неї розрахунків, якісна оцінка факторів не врахованих математичною моделлю, аналіз і синтез результатів кількісної та якісної оцінок і, нарешті, прийняття рішення [9].

Як свідчить світова практика, моделювання динамічних нелінійних систем проводиться на основі використання багатовимірних диференціальних рівнянь, різницевих рівнянь, математичного апарату клітинних автоматів, математичного апарату теорії катастроф, математичного апарату теорії самоорганізованої критичності, стохастичних диференціальних рівнянь Ланжевена та Іто-Стратоновича, аналізу систем з хаосом і реконструкції стійких станів (аттракторів) по тимчасових рядах. При розв’язанні задач комплексної оцінки фактів та подій доцільним є використання системного методу багатокритеріальної оптимізації [10].

На підставі з’ясування завдання, усвідомлення мети дій, має бути визначений чисельний критерій оцінки або показник ефективності (цільова функція).

Основний принцип вибору показника ефективності – його суворі відповідність меті, яка повинна бути досягнута в результаті виконання завдання. Показник ефективності, таким чином, повинен бути мірою досягнення мети дій, мірою успішності виконання завдання.

Відповідно, з огляду на “сетєцентричний” характер, застосування побудови математичної моделі “інформаційної війни” містить перспективу, шляхом залучення сучасних АСУ, побудови тривимірного мультимедійного відображення процесів, впроваджувати найсучасніші засоби та системи управління як у військовому, так і в

громадському секторі суспільства. Ефективно протидіяти правопорушенням в інформаційній сфері чи навіть їх упереджувати.

### **Висновки.**

У роботі розглянутий метод, використовуючи який можливо в сучасних умовах сформулювати актуальний понятійний апарат, ефективно протидіяти правопорушенням в інформаційній сфері, в певних випадках – їх упереджувати.

Вважаємо, що подальший розгляд цієї тематики має перспективу в разі побудови математичної моделі зазначених явищ та процесів і створення, на основі теорії складних систем, при допомозі сучасних засобів програмного забезпечення, ІТ і ГІС технологій, функціонуючої тривимірної динамічної моделі процесів “інформаційної війни”. Таке рішення може надати можливості дослідникам та керівникам розглядати різноманітні версії моделей розвитку сучасних історичних процесів в реальному часі і просторі, включно з впливом на них змін природного середовища, динаміка розвитку якого з’ясована та доведена інструментально-аналітичними методами.

### **Використана література**

1. Окинавская хартия глобального информационного общества. – Режим доступа : [//www.zakon2.rada.gov.ua/laws/show/998\\_163](http://www.zakon2.rada.gov.ua/laws/show/998_163)
2. P.S. Breivik (Patricia Senn) “Education for the information age”, D.W. Farmer and T.F. Mech, eds., *New Directions for Higher Education*, № 78. Summer 1992.
3. Венская декларация о преступности и правосудии : ответы на вызовы XXI века. – Режим доступа : [//www.un.org/ru/documents/decl\\_conv/declarations/vendec.shtml](http://www.un.org/ru/documents/decl_conv/declarations/vendec.shtml)
- Руководство Организации Объединенных Наций по предупреждению преступлений, связанных с применением компьютеров, и борьбе с ними // *Международный обзор уголовной политики*. – 1994. – № 43, 44. – (Нью-Йорк : ООН).
4. Wolfowitz P. Remarks at a conference on defence transformation, sponsored by Heritage Foundation. 2004. February 27. – Режим доступа : [//www.blueshift.nu/doc/Dorfer\\_AmericasGrandStrategy\\_2005\\_FOI.pdf](http://www.blueshift.nu/doc/Dorfer_AmericasGrandStrategy_2005_FOI.pdf)
5. Arquilla J., Ronfeldt D. The advent of netwar // *Networks and netwar*. – Santa Monica, 2001 / RAND.
6. Arquilla J., Ronfeldt D. The emergence of noopolitik. Toward an American information strategy. – Santa Monica, 1999. – P. 41 / RAND.
7. Богданович В.Ю. Теоретические основы анализа проблем национальной безопасности государства в военной сфере : монография. – К. : Основа, 2006. – 296с.
8. Петрик В.М., Прокоф’єва К.О. До питання про застосування методів НЛП у спеціальних інформаційних операціях // *Інформаційна безпека : людина, суспільство, держава*. – 2009. – № 2(2). – С. 71-76.  
Петрик В.М., Прокоф’єва К.О. Застосування методів НЛП із метою подолання впливу посттравматичного синдрому на особистість // *Сучасні інформаційні технології у сфері безпеки та оборони*. – 2010. – № 2(8). – С. 47-52.
- Петрик В.М., Черненко О.Є. Швидка зміна переконання за допомогою нейролінгвістичного програмування // *Сучасні інформаційні технології у сфері безпеки та оборони*. – 2011. – № 3(12). – С. 81-85.
9. Коллинз Г. Структурные методы разработки систем : от стратегического планирования до тестирования / Г. Коллинз, Дж. Блей : [пер. с англ.] ; под ред. и с предисл. В.М. Савинкова. – М. : Финансы и статистика, 1986. – 264 с.
- Остах Ю.П., Невольниченко А.І., Рома О.М. Принципи імітаційного моделювання “бойових систем” у сучасній операції // *Сучасні інформаційні технології у сфері безпеки та оборони*. – 2010. – № 2(8). – С. 34-39.
10. Скурихин В.И. Итеративно-табличные автоматы : монография / В.И. Скурихин, Л.С. Житецкий, Н.М. Проценко. – К. : Наукова думка, 1977. – 168 с.

Абчук В.А. Справочник по исследованию операций / В.А. Абчук, Ф.А. Матвейчук, Л.П. Томашевский. – М. : Воениздат, 1979. – 368 с.

Ламперти Дж. Случайные процессы. Обзор математической теории / Дж. Ламперти : [пер. с англ.]. – К. : Вища школа. 1983. – 224 с.

Кузьмин С.З. Основы проектирования систем цифровой обработки радиолокационной информации / С.З. Кузьмин. – М. : Радио и связь, 1986. – 352 с.

Рябчун С.Г. Типові математичні моделі на основі мереж Петрі, що застосовуються для формалізації паралельних процесів у системі моніторингу високопродуктивних кластерних обчислювальних систем // Сучасні інформаційні технології у сфері безпеки та оборони. – 2010. – № 2(8). – С. 17-22.

Шуренок В.А., Корнієнко В.І., Бовсуновський В.Ю. Методика врахування узгодженості експертної інформації при визначенні режимів роботи багатофункціональної радіостанції // Сучасні інформаційні технології у сфері безпеки та оборони. – 2010. – № 2(8). – С. 29-34.

Соколовська А.В., Томченко О.В. Використання методів системного аналізу для оцінки та прогнозу зміни стану екосистем : зб. тез доповідей XVII міжнарод. наук.-практич. конфер. “Екологія. Людина. Суспільство” ; укладач Д.Е. Бенатов. – К. : НТУУ “КПІ”, 2014. – С. 55-56.

Федоровский А.Д., Якимчук В.Г., Боднар Е.Н., Козлов З.В. Оценка эффективности космических систем ДЗЗ на основе метода анализа иерархий // Косм. наука і технологія. – 2005. – Т. 11. – № 3/4. – С. 75-60.

~~~~~ \* \* \* ~~~~~