

УДК 621.396

Ткаченко В.А., к.в.н.;

Рогов П.Д., к.т.н.;

Бухало Л.В.

Центр воєнно-стратегічних досліджень Національного університету оборони України.

Захист інформаційних ресурсів Сектору безпеки і оборони держави як фактор забезпечення інформаційної безпеки України

Защита информационных ресурсов Сектора безопасности и обороны государства как фактор обеспечения информационной безопасности Украины

Protection of Information Resources of the Security and defense sector as a factor of providing of information security of Ukraine

Резюме. Проведено аналіз публікацій щодо класифікації та сутності поняття “інформаційні ресурси”. Встановлено взаємозв’язок між складовими Сектору безпеки і оборони держави та сферами впливу національної безпеки держави. Визначено необхідність створення системи комплексного захисту інформаційних ресурсів воєнної сфери.

Ключові слова: інформаційна безпека, інформаційні ресурси, Сектор безпеки і оборони держави.

Резюме. Проведен анализ публикаций относительно классификации и сути понятия “информационные ресурсы”. Установлена взаимосвязь между составляющими Сектора безопасности и обороны государства и сферами влияния национальной безопасности государства. Определена необходимость создания системы комплексной защиты информационных ресурсов военной сферы.

Ключевые слова: информационная безопасность, информационные ресурсы, Сектор безопасности и обороны государства.

Resume. Analysis of publications on the classification and the nature of "information resources." The relation between the components of the security sector and influence of national security. The necessity of creation of system of comprehensive protection of information resources of military sphere is defined.

Keywords: information security, information resources, the Security and defense sector of the state.

Постановка проблеми

В XXI столітті рівень розвитку та безпека інформаційного середовища стали найвагомішими факторами в усіх сферах національної безпеки. Її забезпечення з використанням грамотно сформульованої національної інформаційної політики значною мірою сприяє досягненню успіху у виконанні завдань в політичній, воєнній, економічній, соціальній та інших сферах державної діяльності. Разом з тим, сьогодні ніяка сфера (предметна діяльність) людей не може бути ефективно організована без відповідної системи інформаційного забезпечення цієї діяльності. Для забезпечення інформаційної підтримки конкретного виду діяльності людей організується (створюється) відповідна інформаційна

інфраструктура [1]. Невід’ємними складовими інформаційного середовища України є інформаційні ресурси (ІР), інформаційна інфраструктура та інформаційні технології, що входять до національного інформаційного потенціалу.

Державна політика України у сфері інформаційної безпеки спрямована на накопичення та захист національних ІР, розробку та впровадження сучасних безпечних інформаційних технологій, побудову захищеності інформаційної інфраструктури.

Останнім часом визначальної ваги інформаційна безпека набуває у воєнній сфері. Безпосередньо у військовій справі рівень інформаційного потенціалу все більшою мірою обумовлює оперативність прийняття рішень,

структуру та якість озброєнь, оцінку рівня їх достатності, дієвість пропаганди, ефективність дій союзників і власних збройних сил і, в підсумку, результат збройного протистояння. Важливим фактором захисту інформаційної безпеки держави у воєнній сфері має стати захищеність інформаційних ресурсів.

Аналіз джерел

У відомих публікаціях кількість робіт, присвячених проблемі висвітлення сутності, класифікації, систематизації ІР, обмежена. Найбільш фундаментальною є [2].

Відповідно до [3] народжується нове постіндустріальне інформаційне суспільство, в якому знання (наука) стає безпосередньо соціальною (виробничою) силою. Це досягається завдяки інформаційному, точніше, інформдинамічному механізму перетворення знання в ІР і останнього в матеріальну силу. “Інформаційне суспільство – це суспільство, структура, технічна база і людський потенціал якого пристосовані для оптимального перетворення знань в ІР і переробки його з метою переведу із пасивних форм (книжки, статті, патенти тощо) в активні (моделі, алгоритми, програми, проекти тощо)”. Але особливе значення для активізації інформаційного потенціалу суспільства має створення сучасних баз знань. Наука (нові знання) стають соціальною силою, втілюючись в практичний досвід широких мас, а також матеріалізуючись в новій техніці, технологіях, оргсистемах, продуктах і послугах.

Проблемам сутності визначення фундаментальних понять інформації присвячене наукове дослідження [4]. Автори стверджують,

що фундаментальним напрямком створення та розвитку єдиного інформаційного простору України у воєнній сфері є еволюційна побудова та підтримка дієздатності основного (бойового) інформаційного простору України у воєнній сфері. Його достатність забезпечується результатами виконання необхідного переліку завдань, що гарантують формування, використання та розповсюдження ІР в інтересах досягнення переваги над противником.

Отже, аналіз джерел свідчить про те, що практичного змісту проблема інформаційної безпеки у світі набула в останні 20 років, а тому сьогодні вона потребує окремого теоретичного, наукового осмислення, починаючи із визначення сутності цього поняття, зокрема базової категорії “інформаційні ресурси”.

Метою статті є визначення сутності поняття ІР, класифікація цього поняття, встановлення взаємозалежності між захистом ІР Сектору безпеки і оборони держави (СБОД) та інформаційною безпекою держави і обґрунтування необхідності створення системи комплексного захисту ІР.

Виклад основного матеріалу

Національна безпека України має загальним компонентом або складовою – сферу (сектор) воєнної безпеки. Як складова національної безпеки вона також має відповідні підсистеми (сфери): політичну, економічну, воєнну тощо. З огляду на це важливим є встановлення взаємозалежностей між складовими інформаційного середовища СБОД та відповідними сферами національної безпеки держави, як наведено на рис. 1.

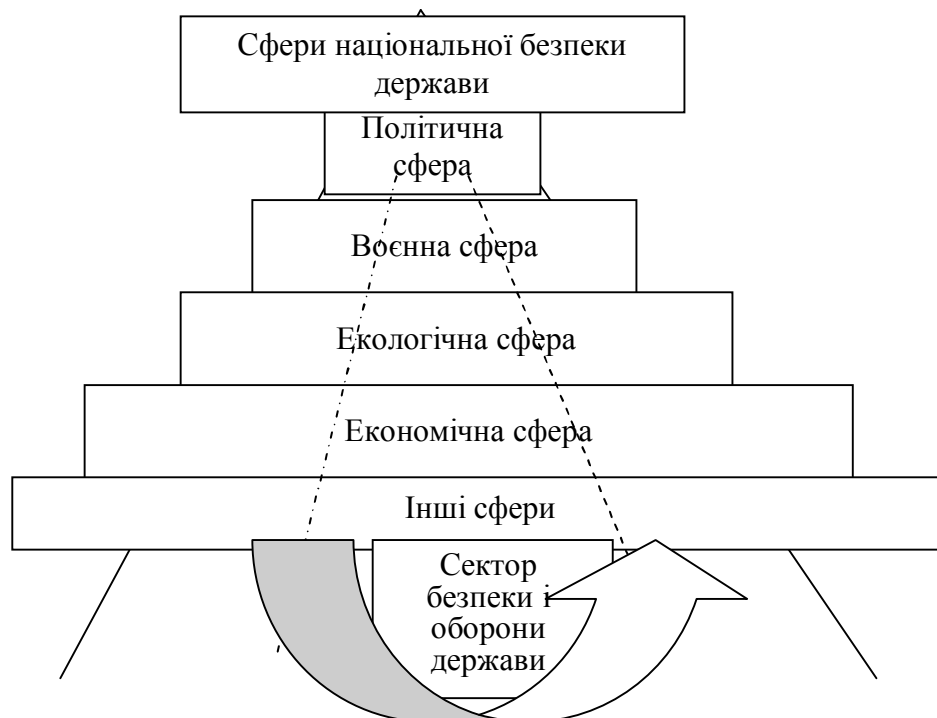


Рис. 1. Взаємозв'язок Сектору безпеки і оборони держави із сферами впливу національної безпеки держави

Захист ІР – одне із пріоритетних завдань національної безпеки України, є важливою складовою державної інформаційної політики. Разом з цим ІР та інформаційний простір держави – основні об'єкти забезпечення інформаційної безпеки держави. Чинне законодавство не встановлює повного юридичного трактування складових ІР. Не визначені критерії віднесення ІР до категорії державних та недержавних. Таке становище створило і надалі створюватиме труднощі щодо формування системи національних ІР, управління цією системою, а також у правовому оформленні функцій, пов'язаних з володінням, використанням і розпорядженням ІР.

На основі інформаційного коректувального супроводження матеріально-енергетичних процесів у суспільстві зароджуються основні потоки евристичної інформації, яка потребує обробки і використання. Що стосується неповноти інформаційних циклів, які охоплюють лише стадії передачі, збору даних, діагностики, інформування, то вони стають дійсно зрозумілими лише при співвіднесенні з повним інформдинамічним процесом (циклом). Інформація як повідомлення деяких відомостей не має самостійної цінності. Її значення для одержувача визначається приростом його знань, співвіднесених з певною метою, або, якщо говорити про кінцевий інформаційний результат, величиною зниження ентропії об'єкту, що розглядається. В новому інформаційному суспільстві наука виступає безпосередньо виробничою силою. Формою безпосередньої участі знань, що виробляються наукою, у виробничому процесі є інформація, точніше ІР, а механізмом ефективної взаємодії наукового виробництва – інформаційний механізм. Тобто, ІР – це необхідна і суттєва проміжна ланка між знанням (наукою) і дією (матеріальним результатом), яку не можна залишити поза межами теорії відтворення.

ІР – інтелектуальний ресурс, фактор колективної творчості, і головна складність в розумінні його природи та функцій полягає в розкритті механізму переходу “знань в силу”, способів його впливу на матеріальні фактори прогресу.

Поняття ІР зароджується на шляху об'єднання формально-логічного і когнітивного підходів. ІР в своєму визначенні

має дві нерозривні складові: формально-логічну (інформаційну) і семантичну (когнітивну). Перший аспект цього фундаментального поняття, а саме формально-логічна сторона, формується в результаті узагальнення практики комп'ютеризації і розвитку інженерних знань. В основі методів використання представлення знань – перший аспект поняття ІР – полягають, головним чином, математична формалізація і логічна повнота. Навпроти, когнітивний підхід базується на розумінні процесу усвідомлення будь-чого людиною, тому представленню знань у даному випадку притаманна швидше виразність, аніж математичні витонченість і строгість. Отже, ІР можна розглядати як “симбіоз” знання та інформації.

Особливого значення набуває поняття “дані” – це відомості про предмети чи окремі факти і про значення їх атрибутів або характеристик. З урахуванням наведених понять можна говорити, що ІР – це легкодоступні для безпосереднього використання дані і знання.

Основна особливість інформаційних процесів полягає в обов'язковій взаємодії трьох елементів: джерела, канали зв'язку, одержувачі повідомлень. Першим пов'язав інформаційну ємність сигналу із середовищем зв'язку Шеннон. Він також поставив вагу повідомлення у залежність від характеристик джерела, каналу і одержувача [5].

Перетворення знань в ІР залежить від можливостей їх кодування, розподілення і передачі.

До особливостей ІР належить:

– ІР практично невичерпний, по мірі розвитку суспільства й інтенсифікації процесу використання знань їх запаси – не зменшуються, а навпаки – ростуть;

– по мірі використання ІР не зникає, а зберігається і навіть збільшується (за рахунок конструктивної трансформації отриманих повідомлень з урахуванням досвіду, місцевих умов тощо);

– він не самостійний і сам по собі має лише потенційне значення та, з'єднуючись з іншими ресурсами, він проявляється “кінетично” – як рушійна сила; - ефективність його використання пов'язана з непервинним (повторним) виробництвом знань, інформаційна взаємодія дозволяє отримати нове знання ціною значно менших витрат у порівнянні з витратами праці, енергії, часу на його пряме генерування;

– IP виступає формою безпосереднього включення науки, в тому числі теоретичних досліджень, до складу виробничих сил;

– виникає IP в результаті не просто розумової праці, а її творчої частини.

Перед людством стоїть велетенська за своєю важливістю і складністю проблема: вилучити максимум інформації із накопичених за всю історію повідомлень та перетворити її в активно функціонуючий ресурс. Мова йде про перетворення книжкових описів й інших розсіяних знань в діючі програми і алгоритми. Це частина робіт із формування IP.

За значущістю IP діляться на стратегічні, тактичні і оперативні [6].

Стратегічні IP – це ресурси, що забезпечують перманентний процес формування менталітету нації як найбільш значущого чинника сталого прогресивного розвитку країни. До складу стратегічних IP мають надходити перетворені у легкодоступну численним користувачам, в тому числі і в електронну форму світоглядні, культурологічні, історичні, правові та інші розділи гуманітарних і фундаментально-природничих знань. У воєнній сфері до стратегічних IP можна віднести воєнну доктрину, закони, що регламентують воєнну діяльність, фундаментальні положення воєнної безпеки тощо.

Тактичні IP включають прикладні науково-технічні, економічні, екологічні, демографічні й інші знання, перетворені в ресурс та необхідні для забезпечення розв'язання в поточному періоді проблем, наприклад, поточних проблем інформаційної чи воєнної безпеки. У воєнній сфері – це сукупність основних положень оперативного мистецтва і тактики родів військ, це воєнно-прикладні знання, що одержуються курсантами і слухачами військових навчальних закладів, статuti, настанови тощо. Це також математичне і програмне забезпечення АСУ та інформаційних систем воєнного призначення.

Оперативні IP – це поточна ділова, комерційна й інша довідкова інформація, що орієнтована на задоволення щоденних потреб у різних сферах діяльності. Для воєнної сфери – це відомості воєнного характеру, які добуваються (отримуються) чи створюються під час розвідки, збору інформації, інформаційної роботи штабів та іншої інформаційної діяльності, а також інформація, що циркулює в АСУ воєнного

призначення, по каналах взаємодії, в інформаційних системах різного рівня, у тому числі і в системах технічної розвідки – оперативні директиви, доповіді, донесення тощо.

Нові технології XXI ст. змінили взаємовідносини між країнами, форми і способи ведення збройної боротьби. Інформаційні війни є реальністю, суспільство повинно знати про неприпустиме ігнорування цього. Країни, позбавлені стратегії щодо забезпечення власної інформаційної безпеки, приречені опинитися на узбіччі світової цивілізації. Особливе значення має проблема захисту (збереження) IP кожної окремої країни.

Відповідно до міжнародних критеріїв IP можна класифікувати за трьома категоріями.

1. Життєво важливі, тобто пов'язані з виживанням і безпекою нації, з її “генетичною” пам'яттю, без захисту якої ми втратимо ідентичність, припинимо своє існування. Вони аж ніяк не можуть бути предметом торгу, й для їхнього захисту повинні залучатися всі наявні ресурси нації.

2. Важливі, які здатні справляти відчутний вплив на добробут нації та характер міжнародних відносин.

3. Гуманітарні, що пов'язані з широким спектром міжнародних проблем, які безпосередньо не зачіпають тріади – “свобода – виживання – процвітання”, але стратегічно вигідні державі для позитивного позиціонування себе як всередині країни, так і на міжнародній арені.

Автори поділяють думку військових фахівців [4], що у воєнній сфері захист IP є основою обороноздатності країни, безпосередньо пов'язаний із забезпеченням інформаційної безпеки СБОД.

До категорій інформаційної безпеки відносяться:

- інформаційний ресурс (IP) воєнної сфери – наявний обсяг даних та інформації, доступних для елементів інформаційної інфраструктури СБОД в інтересах здійснення її суб'єктами функцій управління. З точки зору використання IP воєнної сфери поділяється на два основні види:

- статичний IP, як документована та структурована сукупність знань військового характеру;

– динамічний ІР, як інформація або дані військових систем реального часу, а також ситуативний інтелект людини – військового оператора, який реалізується у формі поточних усних інформаційних повідомлень або команд (розпоряджень) підлеглим та рішень для власних дій, – документуючись, динамічний ІР переходить в розряд статичного;

- інформаційний простір воєнної сфери – інтегроване інформаційне середовище, що створюється інформаційною інфраструктурою СБОД і складається із основного (бойового) інформаційного простору, інформаційного простору сектору ресурсного забезпечення та простору інформаційного захисту, у якому здійснюються усі процеси формування, використання і розповсюдження ІР в інтересах управління військовим будівництвом, підготовкою збройних формувань та інших суб'єктів СБОД до війни (оборони), а також для досягнення інформаційної переваги над противником та управління противником (його діями) у ході воєнного конфлікту.

Особливим видом є комунікативний ІР як сукупність структурованих даних або інформаційних продуктів, що забезпечують зв'язок різних інформаційних конструкцій (обрисів, думок, уявлень) та процесів, які можуть мати характер як статичного, так і динамічного. Більш наочно це розкривається на рис. 2.

Щодо сутності ІР у воєнній сфері. Для вирішення проблеми забезпечення інформаційної безпеки у воєнній сфері необхідно виходити із того, що поняття “воєнна сфера” є сферою діяльності СБОД, спрямованої на захист її національних інтересів від зовнішніх загроз, саме тієї багатопрофільної діяльності держави, яка пов'язана із підготовкою та веденням війни з можливим зовнішнім агресором національними силами і засобами при домінуючій ролі Збройних Сил України; потрібно розуміти сутність того ІР, який є функціонально важливим для діяльності СБОД, зокрема Збройних Сил України як її базової складової.

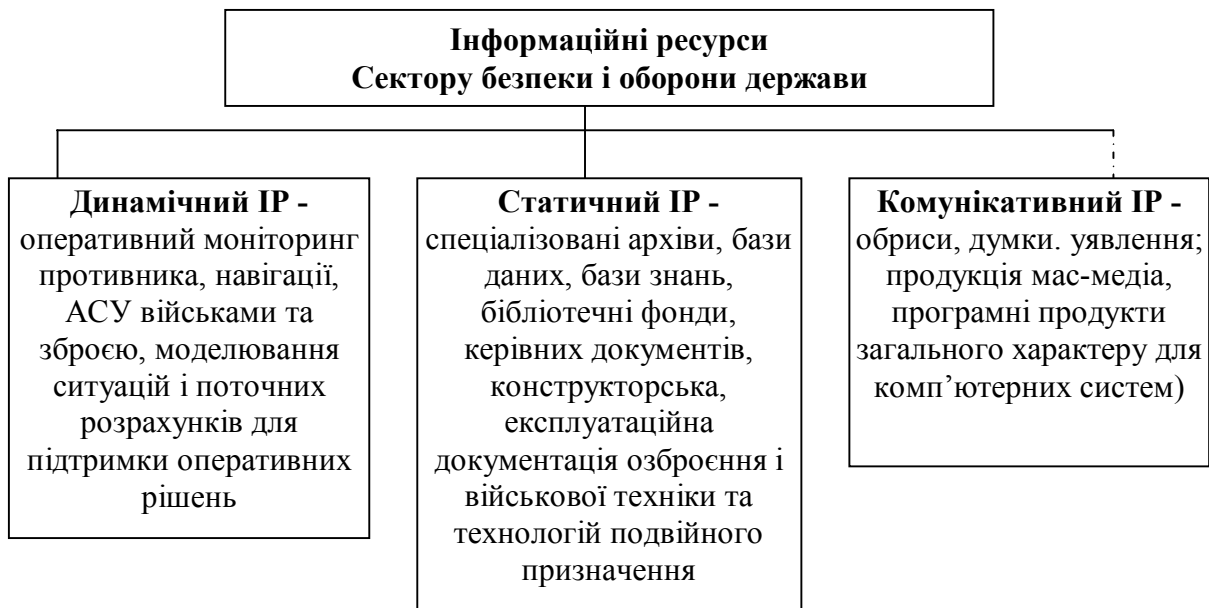


Рис. 2. Класифікація інформаційних ресурсів Сектору безпеки і оборони держави

При цьому, на наш погляд, при визначенні сутності ІР у воєнній сфері слід брати за основу ст. 53 Закону України “Про інформацію” [7], якою визначається, що “інформаційний ресурс України складає вся належна їй інформація, незалежно від змісту, форми, часу і місця створення”. Але тут необхідно зауважити, що погодитись із визначенням у цьому ж законі поняття інформації як “документованих та публічно

оголошених відомостей” для воєнної сфери неможливо, оскільки у цій сфері діяльності надзвичайно важливе значення, поряд з іншим, має інформація реального часу (моніторингу навколишнього простору, навігації, цілевказівки, усні розпорядження і команди), на основі якої приймається рішення незалежно від того, документується вона чи ні. Звідси виходить, що крім потреби внесення відповідних змін у Закон України “Про

інформацію”, необхідно розуміти, що на рівні Збройних Сил України і в цілому всього СБОД загальний (сукупний) ІР для забезпечення діяльності у воєнній сфері складається із сукупності інформаційних продуктів, які мають характер як статичного документованого ІР, так і динамічного недокументованого ІР.

Очевидно, що сутність інформаційної безпеки України у воєнній сфері, системоутворюючим ядром якої є інформаційна інфраструктура Збройних Сил України та Міністерства оборони України є не захищеність ІР від різноманітних інформаційних впливів, а забезпечення процесу ефективного формування та використання національного ІР в інтересах виконання завдань СБОД (захисту національних інтересів України від зовнішніх загроз, в першу чергу, захисту державного суверенітету, територіальної цілісності, недоторканості державного кордону та недопущення втручання у внутрішні справи України).

Отже, нагальною проблемою сучасних Збройних Сил України та Міністерства оборони України щодо забезпечення інформаційної безпеки України у воєнній сфері є врахування процесів формування і використання як статичної, так і динамічної складових ІР при їх всебічному захисті для ефективного функціонування СБОД.

З метою забезпечення інформаційної безпеки у воєнній сфері необхідно створення та активний розвиток єдиного інформаційного простору України, його всебічний захист від несанкціонованого доступу до наявних ІР та зовнішнього руйнівного впливу.

Для досягнення інформаційної переваги над противником, відповідно до [4], формування, використання і розповсюдження ІР СБОД забезпечується завдяки:

- інформатизації суб'єктів сфери СБОД, ефективного функціонування Єдиної АСУ Збройних Сил України, базами даних інших суб'єктів СБОД;
- створенню бази імітаційного моделювання процесів збройної боротьби;
- створенню сучасної системи зв'язку і обміну даними між усіма ланками військового управління;
- еволюційного створення комплексу взаємопов'язаних моніторингових систем;
- удосконалення засобів дистанційного спостереження противника;

– запровадження системи формування та використання спеціальних ІР з метою активного інформаційного тиску на противника шляхом заходів оперативного маскування, інформаційно-психологічного впливу, порушення роботи його інформаційних систем.

Особливу увагу слід зосередити на розробці теорії інформаційних операцій та її впровадження в практику подальшого реформування Збройних Сил України.

Щодо статичних ІР СБОД – матеріально-технічних, фінансових, кадрових, медичних. Постає необхідність створення відомчих і міжвідомчих електронних бібліотек, автоматизованої системи управління адміністративно-господарським процесами Збройних Сил України, встановлення технічних умов і регламенту для вертикального-горизонтального доступу до статичних ІР суб'єктів СБОД. Оскільки комп'ютерні системи тепер безпосередньо інтегровані в інформаційні інфраструктури сучасного суспільства, засоби захисту повинні враховувати сучасні форми подання інформації (гіпертекст, мультимедіа тощо). Це означає, що системи захисту повинні забезпечувати безпеку на рівні ІР, а не окремих документів, файлів або повідомлень [8].

Висновки. В результаті розглянутого вище для вирішення завдань забезпечення інформаційної безпеки СБОД пропонується:

1. Створити орган координації політики і заходів щодо забезпечення інформаційної безпеки у воєнній сфері (з функцією взаємодії з визначеними суб'єктами СБОД). В основу задач такого органу необхідно буде закласти вірне розуміння сукупного ІР у воєнній сфері, механізми його продукування і використання та концептуальні положення, які із цього впливають.

2. Забезпечити взаємодію у кризових ситуаціях елементів системи оперативного моніторингу, які пов'язані з формуванням динамічної складової ІР.

3. Зосередити зусилля на захищеності ІР активними чи пасивними контрзаходами, можливості відновлення ІР у разі впливу протидіючої сторони, поглибити вивчення властивостей ІР певних класів із метою підвищення ефективності оперування ними на всіх етапах їх життєвого циклу.

4. Запровадити та постійно вдосконалювати систему статичного IP сектору ресурсного забезпечення суб'єктів СБОД.

Вищенаведене зумовлює необхідність проведення більш ґрунтовних досліджень з метою визначення потреб отримання та використання необхідних IP СБОД, а саме: створення елементів інформаційної інфраструктури воєнної сфери, які продукують необхідні IP; розробки засобів та процесів використання IP; забезпечення захисту IP. Все це буде можливо у разі створення системи комплексного захисту IP, обґрунтування шляхів створення та розвитку якої є, зокрема, завданням науково-дослідних підрозділів Міністерства оборони України.

1. СПИСОК ЛІТЕРАТУРИ

2. Терминологические зазоры на путях военной информатизации / [Голубев Ю.Н., Голубев Ю.Н., Гринь В.Р., Ширманов А.В.] // Военная мысль. – 2012. – №6. – С. 44 – 53.
3. Рось А.О. Інформаційні ресурси: сутність і класифікація / Рось А.О., Пустовіт С.М. Науково-технічний збірник. Вип. 3. – К.: ННДЦ ОТ і ВБ України, 1999. – 200 с.
4. Каньгин Ю.М. Основы теоретической информатики / Каньгин Ю.М., Калитич Г.И. – К.: Наукова думка, 1990. – 230 с.
5. П.М. Сніцаренко. Витоки і сутність інформаційної безпеки у воєнній сфері та проблеми питання її забезпечення / П.М. Сніцаренко, І.В. Вещицький // Національна безпека: український вимір: щокв. наук. зб. – К., 2009. – Вип. 5(24). – С. 23 – 33.
6. Шеннон К. Работы по теории информации и кибернетики / Шеннон К. – М.: ИЛ. 1958. – 321 с.
7. Информатизация и моделирование в развитии Украины – Информатизация процессов экономического развития Украины. / [Рубан В.Я., Калитич Г.И., Широков В.А., Рось А.А., Майданюк Г.Я., Горбаток Н.И.] Сб. научных трудов. – ГосНИИ информатизации и моделирования экономики Минэкономки Украины. 1994. – С. 5 – 28.
8. Закон України “Про інформацію” №2657 – 12 від 02.10.1992 року.
9. В.М. Богуш. Основи інформаційної безпеки держави: Вступ до спеціальності / Богуш В.М., Юдін О.К. – Харків: Консум, 2004. – 384 с.

Рецензент: Сніцаренко П.М. – к.т.н., с.н.с., ЦВСД НУО України.

Поступила в редакцію 17.04.13