УДК: 316.77:32]:323(477)

Теоретичні аспекти інформаційних війн та національна безпека

А.В. ШУМКА,П.П. ЧЕРНИК
Академія сухопутних військ імені гетьмана Петра Сагайдачного, м. Львів, Україна,
E-mail: andrii_shumka@ukr.net

Авторське резюме

Широкий та всебічний аналіз методів проведення інформаційної війни для формування дієвого механізму протидії має надзвичайно актуальне значення.

Інформаційна війна – дії, що вчиняються для досягнення інформаційної переваги у підтримці національної воєнної стратегії через вплив на інформацію та інформаційні системи противника при одночасному гарантування безпеки власної інформації і інформаційних систем. На сьогодні термін «інформаційна війна» використовується в двох площинах: у широкому розумінні – для визначення протиборства в інформаційній сфері в засобах масової інформації для досягнення різних політичних цілей; у вузькому розумінні – для визначення воєнного протиборства, у військовій інформаційній сфері для досягнення односторонніх переваг в отриманні, зборі, обробці та використанні інформації на полі бою.

Дії, пов'язані із забезпеченням інформаційної безпеки, мають включати: спостереження, аналіз, оцінку і прогноз загроз та небезпек; відпрацювання стратегії і тактики, планування попередження нападу, зміцнення потенційних зв'язків, підсилення ресурсів забезпечення інформаційної безпеки; відбір сил і засобів протидії, нейтралізації, недопущення нападу, мінімізації шкоди від нападу; дії із забезпечення інформаційної безпеки; управління наслідками інциденту (кібератаки, інформаційні операції, інформаційні війни).

Організація ефективної системи забезпечення інформаційної безпеки передбачає централізоване управління із конкретними функціями, які забезпечують моніторинг і контроль за всіма компонентами національного інформаційного простору.

Ключові слова: інформаційна війна, інформаційна безпека держави, національна безпека в інформаційній сфері.

Theoreticalaspects ofinformation war and national security

A.V. SHUMKA, P.H. CHERNYK
Army Academy named after hetman Petro Sahajdachnyj, Lviv, Ukraine,
E-mail: andrii_shumka@ukr.net

Abstract

A wide and comprehensive analysis of methods of conducting information war to create an effective mechanism of counteraction has extremely important significance.

Information warfare - acts committed to achieve information superiority in support of national military strategy due to the impact of information and information systems enemy while ensuring the security of its own information and information systems. Today the term «information war» is used in two areas: in the broadest sense - to determine confrontation in the information sphere in the media to achieve various political goals; in a narrow sense - to determine the military confrontation, military information sector to achieve unilateral advantages in obtaining, collecting, processing and using information on the battlefield.

Actions connected with maintenance of information security should include: observation, analysis, evaluation and prognosis of threats and hazards; working out strategy and tactics, planning attack prevention, strengthening of potential relationships, gain resources information security; selection of forces and means opposition, neutralization, prevent attacks and minimize damage from the attack; actions of ensuring information security; managing the consequences of the incident (cyber attacks, information operations, information warfare).

Organization of effective ensuring information security system provides centralized control of specific functions that provide monitoring and control of all components of the national information space.

Keywords: information war, Information security of the state, national security in the information sphere.

Постановка проблеми. Події, що розгорнулися в Україні впродовж останніх півтора року, є найбільшим випробуванням у новітній історії української державності. Сьогодні, внаслідок проведеного Російською Федерацією комплексу спеціальних операцій, наша держава вже втратила частину своєї території – Автономну Республіку Крим. Об'єктивні виклики сепаратизму та іноземного військового вторгнення загрожують Україні новою втратою територій, та, навіть, самої незалежності. Система національної безпеки України виявилась неефективною, слабкою, нездатною протистояти багатовекторній агресії. Разом з тим, принаймні на сьогодні, зі всього арсеналу, що використовує Російська Федерація на фронтах гібридної війни проти України, найбільш ефективною зброєю, що завдає нищівних ударів

Українській державі стала зброя інформаційної війни. Відтак, широкий та всебічний аналіз методів проведення інформаційної війни для формування дієвого механізму протидії цьому виклику в контексті забезпечення національної безпеки держави має надзвичайно актуальне значення.

Аналіз досліджень і публікацій. Відповідних наукових праць на дану тематику чимало. Так, у сучасних вітчизняних та закордонних дослідженнях окремі теоретичні аспекти інформаційних війн та їх вплив на національну безпеку розглядали А.В. Авраменко, Г.С. Лазарев, М.П. Хріпков, З.Бжезинський, Р.Арон, О. Тофлер. Вивченню сутності інформаційних війн з точки зору політології, теорії держави і права, теорії управління та безпекознавства присвячені праці І.Н. Панаріна, Г.Г Почепцова, В.С.Цимбалюка та ін. Однак швидкоплинність процесів у сучасному глобалізованому світі та постійний розвиток новітніх форм і методів ведення інформаційних воєн та відповідне оформлення безпекових основ держави формують гостру необхідність у нових наукових роботах.

Метою дослідження є узагальнення теоретичних аспектів гарантування інформаційної безпеки держави, аналізі сучасних інформаційних війн та джерел загроз національній безпеці в інформаційній сфері.

Виклад основного матеріалу. Отже, у науковій літературі бракує єдиного консолідованого погляду на зміст поняття «інформаційна безпека». Для одних воно відображає стан, для інших процес, діяльність, здатність, систему гарантій, властивість, функцію. Відтак постає необхідність в угрупуванні напрямів визначення аналізованого поняття.

Відповідно до законодавства України, поняття «інформаційна безпека» має таке визначення: «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди державі через неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації» [1].

Розробники концепції інформаційної безпеки центру Разумкова, а також деякі українські дослідники, які вважають за необхідне визначати інформаційну безпеку як стан захищеності. Так, наприклад, Гасеський В.К., Авраменко В.А. визначають інформаційну безпеку як стан захищеності життєво важливих інтересів особи, суспільства та держави, який виключає можливість заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації [3], у той час як Додонов О.Г. визначає інформаційну безпеку як стан захищеності інформаційного простору, який забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави [4].

Аналогічного погляду дотримується і інший російський дослідник Панарін І.М., роблячи більший акцент на ролі політичної еліти, яка може протистояти інформаційному впливу. На його думку, інформаційна безпека – стан інформаційного середовища суспільства і політичної еліти, який забезпечує її формування і розвиток в інтересах керівництва країни, громадян і суспільства [4, с. 234].

Ярочкін В.І. визначає безпеку як «стан захищеності особи, суспільства і держави від зовнішніх та внутрішніх небезпек і загроз, який базується на діяльності людей, суспільства, держави, світового співтовариства з виявлення (вивчення), попередження, послаблення, ліквідації і відбиття небезпек і загроз, здатних загубити їх, лишити фундаментальних матеріальних і духовних цінностей, завдати неприйнятної шкоди, закрити шлях для прогресивного розвитку». Застосування діяльнісного підходу, на наш погляд, є більш адекватним при описуванні інформаційної безпеки, і ми в певній мірі можемо підтримати дане визначення у загальному плані, однак не погодитись із деталізацією напрямів діяльності, які з часом змінюватимуться, а отже, закладатимуть потенціал нестійкості як до самого визначення, так і до функціонування відповідних суб'єктів [12, с. 64].

М.П. Хріпков вважає, що діяльність по забезпеченню особи, суспільства і держави виникає в ході вирішення суперечності між такою об'єктивною реальністю, як небезпека і потребою соціального індивіда, соціальної групи попередити її можливі шкідливі наслідки. Водночас за даного випадку функціонування системи забезпечення інформаційної безпеки зводиться лише до реагування, тоді як превенція лишається поза увагою [11].

Саме тому, на наше переконання, інформаційна безпека становить собою діяльність органів державного управління. Звідси витікає важливий висновок, що слід діяти активно, здійснюючи вплив на джерела інформаційної небезпеки. При цьому щодо змісту інформаційної безпеки доцільно використовувати не поняття «інтереси», а більш фундаментальне поняття «цінності», через те, що у цінностях знаходять вираження інтереси суб'єктів суспільних відносин, зіткнення яких породжує загрози. На сьогодні саме інформаційні війни становлять собою найбільшу небезпеку нормальному функціонуванню системи органів державного управління. Вперше термін «інформаційна війна» з'явився наприкінці 70-х

років XX століття. Він став результатом плідної праці теоретиків збройних сил США і став уживаним після вдало проведеної роботи по знищенню СРСР. Активного застосування даний термін набув під час проведення воєнної компанії США в Іраку у 1991 році, де вперше були не лише застосовані інформаційні технології, а було відкрито наголошено на цьому, що спричинило ще більший резонанс.

Досвід неприділення необхідної уваги даним питанням спричинив розпад СРСР, могутньої держави, яка до 1991 року була єдиним реальним конкурентом США у владарюванні світом. Саме це надає можливість стверджувати необхідність розроблення концепції інформаційного стримування. Події із касетним скандалом у 2001 році, звинувачення у постачанні комплексів радіотехнічної розвідки «Кольчуга» в Ірак у лютому 2004 року, інформаційні протистояння на тлі «газових воєн» та, зрештою,теперішні щоденні інформаційні провокації російських ЗМІ дають усі можливості стверджувати, що в Україні відсутня розроблена на концептуальному рівні концепція забезпечення інформаційної безпеки. Більше того, аналіз сучасної геополітичної обстановки дає нам усі підстави зробити висновок, що проти України здійснюються широкомасштабні інформаційні акції, спрямовані на дискредитацію, дезорганізацію, підрив іміджу та дестабілізацію нашої держави. І передусім цей вилив чиниться на систему забезпечення національної безпеки.

Безперечно, якщо ми говоримо про інформаційну війну, то вочевидь зрозумілим є факт, що даний термін є найбільш спорідненим із воєнними. Тому, коли йдеться про інформаційну війну, слід говорити про існування рішучої і небезпечної діяльності, пов'язаної із реальними бойовими діями. Більше того, в цьому контексті постає необхідність виокремлення декількох підвидів інформаційних війн: кібернетична війна, електронна війна, психотропна війна, штабна війна, психологічна, енерго-інформаційна війна тощо[11, с.224-226].

Таке розуміння інформаційної війни дає можливість погодитись із визначенням поняття інформаційної війни, яке мається у збройних силах США. Отже, інформаційна війна – дії, що вчиняються для досягнення інформаційної переваги у підтримці національної воєнної стратегії через вплив на інформацію та інформаційні системи противника при одночасному гарантуванні безпеки власної інформації та інформаційних систем. Одним з прикладів є існування спеціальної програми запису усіх телефонних дзвінків, що виходять за кордон США на спеціальну апаратуру. За допомогою такої програми усі телефонні дзвінки, що виходять за межі країни, записуються, а потім пропускаються через спеціальний пристрій, який за допомогою пошукових систем за ключовими словами здійснює виявлення та ідентифікацію важливої інформації.

Відтак, існування розвиненої системи інформаційної безпеки закладе фундамент для стійкого функціонування системи державного управління. На думку деяких дослідників, стрімкий розвиток інформаційних технологій спричинить у майбутньому появу нових за змістом видів війн, які відбуватимуться без жодного пострілу. Особливо наголосимо, що сучасні інформаційні війни спрямовані здебільшого на економічну інфраструктуру.

Цілі інформаційної війни є дещо іншими, аніж війни у звичному розумінні: не фізичне знищення противника і ліквідація його збройних сил, а широкомасштабне порушення роботи фінансових, транспортних і комунікаційних мереж і систем, руйнування економічної інфраструктури і підкорення населення країни, що зазнала атаки, волі країни-переможця.

На сьогодні термін «інформаційна війна» використовується в двох площинах: у широкому розумінні — для визначення протиборства в інформаційній сфері в засобах масової інформації для досягнення різних політичних цілей; у вузькому розумінні — для визначення воєнного протиборства, у військовій інформаційній сфері для досягнення односторонніх переваг в отриманні, зборі, обробці та використанні інформації на полі бою (в операції, битві) [8].

Інформаційна війна має наступальні та оборонні складові, одна з найголовніших її цілей – забезпечити особам, які приймають рішення, відчутну інформаційну перевагу у різноманітних конфліктах. Інформаційна війна може бути спрямована проти трьох елементів: комп'ютер; програмне забезпечення; людина.

Крім того, неможливо заперечувати й того факту, що однією з головних цілей та завдань інформаційної війни є придушення в людині морального творчого початку, зміна світогляду.

На міжнародній арені інформаційні війни ведуться між державами та блоками держав; між міжнародними корпораціями, транснаціональними корпораціями і міжнародними фінансовими групами; між міжнародними корпораціями, ТНК і міжнародними фінансовими групами з державами; між терористичними організаціями та державами; між міжнародними корпораціями, ТНК і міжнародними фінансовими групами; між злочинними організаціями; між злочинними організаціями та державами.

Взагалі ж технології інформаційного віку певним чином зрівняли індустріальні, постіндустріальні і доіндустріальні країни: всі вони мають доступ до інструментарію, необхідного для ведення інформаційної війни, а отже виступають як суб'єктами, так і об'єктами інформаційної війни, а отже, і забезпечення внутрішньої інформаційної безпеки.

Слід зазначити, що аналізові змісту по-

няття «інформаційна безпека» зазвичай дослідниками приділяється значна увага, у той час як такі поняття, як небезпека і загроза розглядаються дещо спрощено і здебільшого у звуженому плані, відірваному від контексту поняття «інформаційна безпека» і майже не пов'язаному із контекстом поняття «загроза» в рамках національнобезпекознавства.

Найбільш широко загрози інформаційним ресурсам можна розглядати як потенційно можливі випадки природного, технічного або антропогенного характеру, які можуть спричинити небажаний вплив на інформаційну систему, а також на інформацію, що зберігається в ній.

Виникнення загрози, тобто віднаходження джерела актуалізації певних подій у загрози характеризується таким елементом як уразливість. Саме за наявності вразливості, як певної характеристики системи і відбувається активізація загроз. Безперечно, що самі загрози за своєю суттю є невичерпними, а отже й не можуть бути піддані повному описові у будь-якому дослідженні.

Відповідно до Закону України «Про основи національної безпеки України» до загроз національним інтересам і національній безпеці в інформаційній сфері відносять наступні: прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

До загроз інформаційній безпеці системі управління національною безпекою належать: розкриття інформаційних ресурсів; порушення їх цілісності; збій у роботі самого обладнання [2].

Головна причина поразки, яку зазнав Київ в інформаційній війні навколо березневого протистояння 2014 року у Криму та неефективного протистояння сьогодні на Сході – відсутність будь-якої системної, методичної роботи в інформаційній сфері. Діяльність із забезпечення інформаційної безпеки здійснюється за допомогою різних способів, засобів і прийомів, які у сукупності й складають методи. Метод передбачає певну послідовність дій на підставі конкретного плану.

Виділяють декілька типів методів забезпечення інформаційної безпеки: однорівневі методи будуються на підставі одного принципу управління інформаційною безпекою; багаторівневі методи будуються на основі декількох принципів управління інформаційною безпекою, кожний з яких вирішує власне завдання. При цьому дані технології не пов'язані між собою і спрямовані лише на конкретні чинники інформаційних загроз; комплексні методи — багаторівневі технології, які об'єднані в єдину систему координуючими функціями на організаційному рівні, з метою забезпечення інформаційної безпеки, виходячи з аналізу сукупності чинників небезпеки, які мають семантичний зв'язок або генеруються з єдиного інформаційного центру інформаційного впливу; інтегровані високоінтелектуальні методи – багаторівневі технології, які побудовані за допомогою потужних автоматизованих інтелектуальних засобів з організаційним управлінням [5].

Загальні методи забезпечення інформаційної безпеки активно використовуються на будь-якій стадії управління загрозами. До таких стадій належать: прийняття рішення з визначення сфери та контексту інформаційної загрози і складу учасників процесу протидії; ухвалення загальної стратегії і схеми дій в політичній, економічній, соціальній та інших сферах життєдіяльності; забезпечення адекватного сприйняття загрози та небезпеки у нижчих організаційних ланках системи управління; виділення необхідних політичних, економічних, соціальних, адміністративних і організаційних ресурсів, достатніх для реалізації програми відбиття інформаційної загрози і збереження сталого розвитку інформаційних ресурсів системи управління; трансформація результатів оцінки ризиків у відповідну політику безпеки, включаючи національну.

Специфіка методів, що використовуються, значно залежить від суб'єкта діяльності, об'єкта впливу, а також цілей, що переслідуються. Так, методи діяльності індивіда у зв'язку із його обмеженою можливістю із забезпечення інформаційної безпеки здебільшого зводяться до джерела загрози, апелювання до суспільної думки, а також до держави, яка має вживати рішучих заходів по нейтралізації інформаційних загроз. Саме суспільство часто використовує у своїй діяльності методи соціального регулювання, надання допомоги окремим індивідам і суспільним організаціям, яким спричинена шкода внаслідок виявлення загрози.

Причому, на жаль, слід констатувати, що в нашій країні не на достатньому рівні усвідомлюють небезпеку саме в інформаційній сфері, немає штатних спеціалістів з інформаційної безпеки в органах державного управління, не на достатньому рівні проводиться підготовка відповідних фахівців.

Дуже важливим є застосування аналітичних методів пізнання і дослідження стану суспільної свідомості у сфері інформаційної безпеки. Наприклад, усвідомлення важливості

забезпечення інформаційної безпеки на рівні індивіда, суспільства і організації заважає розповсюджений міф про те, що захист інформації і криптографія одне й те саме. Водночас таке розуміння є наслідком використання застарілих підходів до інформаційної безпеки, коли інформаційна безпека лише ототожнюється із захистом інформації шляхом шифрування.

Нині важливою умовою забезпечення інформаційної безпеки є не стільки секретність, конфіденційність інформації, скільки її доступність, цілісність, захист від різних загроз. Отже, система має відповідно реагувати і гарантувати ефективну діяльність у цьому напрямі.

Іншим завданням захисту є забезпечення незмінності інформації під час її зберігання або передачі, тобто забезпечення її цілісності. Таким чином, конфіденційність інформації, яка забезпечується за допомогою криптографічних методів, не є головною вимогою при проектуванні систем захисту інформації. Таким чином, управління в сфері інформаційної безпеки має здійснюватися на підставі принципу доступності та безпеки. Система забезпечення інформаційної безпеки в першу чергу має гарантувати доступність і цілісність інформації, а її конфіденційність – у випадку необхідності [10].

Втім, не слід плекати надію на створення абсолютної системи інформаційної безпеки, оскільки ми стоїмо, ми переконані, що загроза та небезпека є атрибутивними компонентами системи інформаційної безпеки, отже, їх існування та реалізація, а також негативні наслідки є природним компонентом системи інформаційної безпеки. Саме вони дають змогу побачити недоліки в системі управління інформаційною безпекою і водночас слугують імпульсом до вдосконалення, тобто до розвитку.

Захист інформації не обмежується технічними методами. Для ефективного забезпечення інформаційної безпеки важливим є різноманітні моделі та методи оцінки загроз та небезпек, їх варіативність залежить як від рівня розвитку тієї чи іншої цивілізації, так і від контексту оцінки, що проводиться, наявності всебічних даних по факторах загрози, алгоритму вирахування коефіцієнта ймовірності настання та розміру негативних наслідків. Наявність конкретних даних з цього питання дозволяє достатньо точно визначити ступінь впливу інформаційної зброї, рівень загроз та небезпек.

Основним методом аналізу інформаційних ризиків є кількісний та якісний аналіз, факторний аналіз тощо. Мета якісної оцінки ризиків — ранжувати інформаційні загрози та небезпеки за різними критеріями, система яких дозволить сформувати ефективну систему впливу на них.

Важливим методом забезпечення інформаційної безпеки є також метод критичних сценаріїв. У зазначених сценаріях аналізуються ситуації, коли уявний противник паралізує систему державного управління і відповідно знижує здатність підтримувати державне управління в межах оптимальних параметрів. Причому аналіз подій у світі дає всі підстави стверджувати, що інформаційні війни стають органічною частиною політики національної безпеки багатьох розвинених країн.

Також можна зазначити метод моделювання, за допомогою якого можливе навчання з інформаційної безпеки. Позитивний досвід цього є у США, де на базі однієї з відомих корпорацій постійно проводяться оперативно-дослідницькі навчання, щоб моделювати різні форми інформаційних атак у ході інформаційної війни.

Серед методів забезпечення інформаційної безпеки важливе значення відіграє метод дихотомії. Для протидії загрозам інформаційній безпеці вживаються необхідні заходи як у напряму надання певного впливу на джерело загрози, так і в напряму зміцнення об'єкта безпеки. Відповідно виділяють дві предметні сфери протидії. Одна з них утворюється сукупністю джерел загроз, а інша – сукупністю заходів по забезпеченню інформаційної безпеки об'єкта.

Методи впливу на інформацію у формі повідомлень можна поділити також на електронні та неелектронні. Електронні методи впливу застосовуються у тих випадках, коли повідомлення закріплюються на електромагнітних носіях, котрі призначені для оброблення за допомогою засобів обчислювальної техніки.

Вони полягають у знищенні, викривленні, копіюванні повідомлень, які зберігаються на цих пристроях. Такі дії можуть бути вчинені лише за допомогою технічного і програмного забезпечення. Неелектронні методи за своєю суттю мають той самий зміст, але реалізуються без використання засобів обчислювальної техніки для впливу на повідомлення, закріплення на інших, передусім паперових, носіях інформації.

Методи впливу на інформаційну інфраструктуру можуть бути поділені на інформаційні та неінформаційні. Інформаційні методи впливу орієнтовані на порушення формування інформаційно-телекомунікаційних систем, мереж зв'язку, засобів автоматизації управління, систем автоматизованої обробки інформації і, таким чином, на попередження нанесення шкоди предметам суспільних відносин, що захищаються [7].

Найбільш важливими напрямами діяльності у цій галузі є всебічна оцінка загроз і небезпек, національної вразливості, ідентифікація критичної інфраструктури. У процесі забезпечення інформаційної безпеки важливо розуміти характер, природу, сутність і зміст загроз та небезпек, вміти своєчасно ідентифікувати джерело загрози [6].

Висновки. Аналіз стану забезпечення інформаційної безпеки показує необхідність удо-

сконалення системи адміністративно-правового регулювання інформаційної безпеки. Постає потреба у виробленні нових засобів, методів і способів забезпечення інформаційної безпеки державного управління, моніторинг інформаційного середовища, наявності загроз та небезпек.

Удосконалення забезпечення інформаційної безпеки потребує цілеспрямованого вивчення зарубіжного досвіду організації і проведення інформаційних операцій, методів, засобів здійснення кібератак, а також моделювання інформаційних нападів.

Проведений нами аналіз дає можливість стверджувати, що система гарантування інформаційної безпеки має бути міжвідомчою і ієрархічно організованою, її структура і організація мають відповідати структурі державного управління з чіткою координацією дій окремих сегментів.

Організація ефективної системи забезпечення інформаційної безпеки передбачає централізоване управління із конкретними функціями, які забезпечують моніторинг і контроль за усіма компонентами національного інформаційного простору.

СПИСОК ЛІТЕРАТУРИ:

1. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» // Відомості Верховної Ради України (ВВР), 2007 р., № 12, ст. 102.
2. Закон України «Про захист інформації в автоматизованих системах» від 05.07.94, № 80/94-ВР. – К., 2003.
3. Авраменко А.В., Гасеський В.К. Інформаційна безпека в Україні як складова національної безпеки / А.В.Авраменко, В.К.Гасеський // Зб. наук. праць. УАДУ – К.: Вид-во УАДУ, 2012. – № 18. – С. 9-18.
4. Додонов О.Г. Проблеми організації єдиного інформаційного простору України / О.Г.Додонов // Науково-технічна інформація. – К., 2000. – №3. – С. 14-18.
5. Ібрагімова І.В. Інформаційна політика крізь призму національної безпеки /І.В.Ібрагімова // Зб. наук. праць. УАДУ. – К.: Вид-во УАДУ, 2013. – Вип. 20 – С. 26-40.
6. Лазарев Г.С.Захист інформації в інформаційно-телекомунікаційних системах / Г.С.Лазарев // Національна безпека і оборона. – К.: 2001. – № 1. – С. 80-83.
7. Логінов О.М. Сучасні проблеми забезпечення інформаційної безпеки в контексті формування системи державного управління / О.М.Логінов// Науковий вісник Юридичної академії Міністерства внутрішніх справ: Збірник наукових праць. – 2011. – № 18. – С. 199-204.
8. Мирка О.С., Ніколаєв І.М. Інформаційна війна та інформаційна безпека (огляд думок зарубіжних політологів та воєнних спеціалістів) / О.С.Мирка, І.М.Ніколаєв // Наука і оборона. – № 16. – 2009. – С. 56-58.
9. Панарин И.Н. Информационная война и геополитика / И.Н.Панарин // Изд-во: Русское слово.– М.2009, 466с.
10. Цимбалюк В.С. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права / В.С. Цимбалюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – К. : Вид-во НТУ України «КПІ»,2011. – № 23. С.43-48
11. Хріпков М.П. До забезпечення воєнної безпеки в умовах загрози інформаційної війни / М.П.Хрімов // Наука і оборона : наук.-теорет. та наук.-практ. журнал. – 1999. – № 2. – С. 37-43.
12. Ярочкин В.Н. Информационная безопасность./ В.Н.Ярочкин //Учебник для студентов вузов. – М.: Академический Проект. Фонд «Мир», 2003. – 640 с.

Стаття надійшла до редакції 17.07.2015

REFERENCES:

1. Zakon Ukrainy «Pro Osnovni zasady rozvytku informatsiinogo suspilstva v Ukraini na 2007-2015 roky» (About the main principles of information society development in Ukraine for 2007-2015). *Vidomosti Verhovnoi Rady (VVR),* 2007, no. 12, pp. 102.
2. Zakon Ukrainy «Pro zahyst informacii v avtomatyzovanyh systemah» (About the protection of information in automated systems) vid 05.07.94, no. 80/94-VR. – K., 2003.
3. *Avramenko, A.V., Gaseski, V.K.* Informatsiina bezpeka v Ukraini jak skladova natsionalnoi bezpeky (Information security in Ukraine as part of national security). *Zbirnyk naukovyh prac.* Kyiv, 2012, no. 18, pp. 9-18.
4. *Dodonov, O.G.* Problemy organizacii jedynogo informaciinogo prostoru Ukrainy (The problems of the organization unified information space of Ukraine). *Naukovo-tehnichna informaciia.* Kyiv, 2000, no. 3, pp. 14-18.
5. *Ibrahimova, I.V.* Informatsiina polityka kriz pryzmu natsionalnoi bezpeky. (Information policy through the prism of national security). *Zbirnyk naukovyh prac.* Kyiv, 2013, no. 20, pp. 26-40.
6. *Lazarev, G.S.* Zahyst informacii v informatsiino-telekomunikatsiinyh systemah (Protection of information in telecommunication systems). *Natsionalna bezpeka i oborona.* Kyiv, 2001, no.1, pp. 80-83.
7. *Loginov, O.M.* Suchasni problemy zabezpechenna nformatsiinoi bezpeky v konteksti formuvanna systemy derzhavnogo upravlinna (Modern problems providing information security in the context of state management system forming). *Naukovyi visnyk Yurydychnoii akademii Ministerstva vnutrishnih sprav. Zbirnyk naukovyh prats,* 2011, no. 18, pp. 199-204.
8. *Mirka, O.S., Nikolajev, I.M.* Informatsiina vijna ta informatsiina bezpeka (ohlyad dumok zarubizhnyh politologiv ta vijennyh spetsialistiv) (An information war and information security (review the opinions of for-

eign political scientists and military experts). *Nauka i oborona,* 2009, no.16, pp. 56-58.
9. *Panarin, I.N.* Informatsionaya voyna I geopolitika (Information warfare and geopolitics). *Russkoye slovo,* Moskva, 2009, pp. 466.
10. *Tsymbalyuk, V.S.* Problemy derzhavnoji informatsijnoii polityky: harmonizatsija mizhnarodnogo i natsionalnogo informatsijnogo prava (The problems of state information policy: harmonization of international and national information law). *Pravove, normatyvne ta metrologichne zabezpechennya systemy zahystu informatsii v Ukraini.* Kyiv, 2011, no. 23, pp. 43-48.
11. *Hripkov, M.P.* Do zabezpechennya vojennoji bezpeky v umovah zahrozy informatsijnoii vijny (To ensure military security under the threat of information warfare). *Nauka i oborona: nauk.-teoret. ta nauk.-prakt. zhurnal,* 1999, no. 2, pp. 37-43.
12. *Yarochkin, V.N.* Informatsionnaya bezopasnost (Informational security). *Uchebnik dlya studentov vuzov,* Moskva, 2003, pp. 640.

Шумка Андрій Володимирович – кандидат історичних наук
Академія сухопутних військ імені гетьмана Петра Сагайдачного
Адреса: 79012, м. Львів, вул. Героїв Майдану, 32
E-mail: andrii_shumka@ukr.net

Черник Петро Петрович – кандидат політичних наук, доцент
Академія сухопутних військ імені гетьмана Петра Сагайдачного
Адреса: 79012, м. Львів, вул. Героїв Майдану, 32
E-mail: petro.chernyk@ukr.net

Shumka Andriy Volodymyrovych – PhD in history
Army Academy named after hetman Petro Sahajdachnyj
Address: 32, Gerojiv Majdanu Str., Lviv, 79012, Ukraine
E-mail: andrii_shumka@ukr.net

Chernyk Petro Hetrovych – PhD in political science, associate professor
Army Academy named after hetman Petro Sahajdachnyj
Address: 32, Gerojiv Majdanu Str., Lviv, 79012, Ukraine
E-mail: petro.chernyk@ukr.net