Ю. В. Нестеряк,
кандидат філолологічних наук,
докторант кафедри інформаційної політики та технологій,
Національна академія державного управління
при Президентові України

МІЖНАРОДНІ КРИТЕРІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ: ТЕОРЕТИКО-МЕТОДОЛОГІЧНИЙ АНАЛІЗ

У статті розглядаються міжнародні методи протидії інформаційно-психологічній агресії та інформаційній війні на основі теоретико-методологічного аналізу міжнародних критеріїв інформаційної безпеки. Виокремлено та проаналізовано два основні підходи до дослідження цих критеріїв виходячи з техніко-технологічного та гуманітарного вимірів реалізації інформаційної політики держави.
Взявши до уваги загальноприйняте визначення інформаційної безпеки держави як стану захищеності життєво важливих інтересів особистості, суспільства і держави, йдеться про можливості запобігти шкоди населенню через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки інформаційних технологій; несанкціоноване використання, поширення порушення цілісності, конфіденційності та доступності інформації.
Ключові слова: інформаційна безпека, інформаційна війна, інформаційна вразливість, інформаційна зброя, критерії оцінки інформаційної безпеки.

Yu. V. Nesteryak,
Doctoral Candidate in Philology, Doctoral student of the Iinformation policy and technology Chair, National Academy of Public Administration, Office of the President of Ukraine

INTERNATIONAL CRITERIA FOR INFORMATION SECURITY STATE: THEORETICAL AND METHODOLOGICAL ANALYSIS

This article investigates methods to counter international information and psychological war of aggression on the basis of theoretical and methodological analysis of international criteria of information security. Isolated and analyzed two basic approaches: technical and technological and humanitarian measure implementation of the information policy of the state to ensure the information security of the individual, society and state.
Based on the generally accepted definition of information security of the state as the state of protection of the vital interests of the individual, society and the state, it is a way to prevent damage to the population through: incomplete, untimely, and unreliable information used, the negative impact of information, the negative effects of information technology; unauthorized use, distribution, and violation of the integrity, confidentiality and availability of information.
Key words: information security, information warfare, information vulnerability, information warfare, information security evaluation criteria.

Ю. В. Нестеряк,
кандидат филологических наук,
докторант кафедры информационной политики и технологий, Национальная академия государственного управления при Президенте Украины

МЕЖДУНАРОДНЫЕ КРИТЕРИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА: ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЙ АНАЛИЗ

В статье рассматриваются международные методы противодействия информационно-психологической агрессии и информационной войне на основе теоретико-методологического анализа международных критериев информационной безопасности. Выделены и проанализированы два основных подхода к исследованию этих критериев учитывая технико-технологическое и гуманитарное измерения реализации информационной политики государства.
Исходя из общепринятого определения информационной безопасности государства как состояния защищенности жизненно важных интересов личности, общества и государства, речь идет о возможности предотвратить ущерб населению через: неполноту, несвоевременность и недостоверность используемой информации; негативное информационное влияние; негативные последствия информационных технологий; несанкционированное использование, распространение и нарушение целостности, конфиденциальности и доступности информации.
Ключевые слова: информационная безопасность, информационная война, информационная уязвимость, информационное оружие, критерии оценки информационной безопасности.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими і практичними завданнями полягає в необхідності теоретико-методологічного аналізу міжнародних критеріїв інформаційної безпеки, дослідження маніпулятивних технологій та інформаційних війн, оцінки систем захисту інформаційних ресурсів держави, аналізу ефективності державної

інформаційної політики із забезпечення інформаційної безпеки та захисту життєво важливих інтересів особистості, суспільства і держави.

Аналіз досліджень і публікацій із зазначеної проблеми свідчить, що дослідженням ефективності державної інформаційної політики із забезпечення інформаційної безпеки та захисту життєво важливих інтересів особистості, суспільства і держави з другої половини XX ст. приділяють серйозну увагу відомі зарубіжні вчені У.Боудіш, Н.Вінер, П.Кеннеді, Л.В.Кокс, М.Лібікі, С.Мец, Дж.Стейн, Т.Томас, Е.Тоффлер, С.Хантінгтон та багато інших.

Протидії потенційним загрозам нових інформаційних технологій, аналізу систем захисту національних інформаційних ресурсів, дослідженню маніпулятивних технологій та інформаційних війн присвячено чимало наукових праць російських дослідників, зокрема Л.Войтасика, В.Домарьова, А.Зінов'єва, А.Панаріна, С.Расторгуєва, Г.Рогозіна, В.Сєдньова, В.Щуригіна та інших.

Усе більшу увагу дослідженню інформаційної вразливості людини, суспільства і цивілізації в цілому, виокремленню інформаційних загроз для держави та пошукам оптимальної політики інформаційної безпеки приділяють вітчизняні науковці І.Горбатенко, Т.Гріненко, В.Долгов, О.Литвиненко, Є.Макаренко, А.Мінін, М.Ожеван, О.Петров, Г.Почепцов, О.Старіш, О.Таликін, А.Чічановський, В.Шкляр, А.Юричко та інші.

Метою цієї статті є визначення міжнародних критеріїв оцінки інформаційної безпеки, виокремлення і дослідження техніко-технологічного та гуманітарного вимірів забезпечення інформаційної безпеки, аналіз міжнародних методів протидії інформаційно-психологічній агресії та інформаційній війні.

Виклад основного матеріалу дослідження. З розвитком глобальних інформаційно-комунікаційних технологій наприкінці минулого століття суттєво зросли загрози інформаційній безпеці, і тому виникла об'єктивна нагальна необхідність розробки нових міжнародних критеріїв інформаційної безпеки. Виходячи із загальноприйнятого визначення ***інформаційної безпеки держави*** як стану захищеності життєво важливих інтересів особистості, суспільства і держави йдеться про можливості запобігти шкоди населенню через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки інформаційних технологій; несанкціоноване використання, поширення порушення цілісності, конфіденційності та доступності інформації. При цьому, на думку вітчизняних науковців А.Чічановського та О.Старіша, важливим є збереження збалансованості інтересів особистості, суспільства і держави [5, с. 352]. Якщо інтереси особистості полягають у реалізації конституційного права доступу до інформаційних ресурсів та не забороненого законом їх використання, а також захисту персональних даних, то інтереси суспільства полягають у досягненні суспільної згоди й духовному розвитку суспільства на основі забезпечення інтересів особи, у зміцненні демократії та побудові правової держави. Держава, у свою чергу, украй зацікавлена в розбудові національної інформаційної інфраструктури, реалізації громадянами конституційних гарантій права доступу до інформаційних ресурсів задля збереження непорушності конституційного устрою, суверенітету і територіальної цілісності держави, соціально-політичної та економічної стабільності.

Відповідно до національних інтересів держави формуються внутрішня і зовнішня політики із забезпечення інформаційної безпеки, що потребує довершеніших систем і технологій управління – ***інформаційних технологій (ІТ)***. Однією з таких технологій, очевидно, є сучасні інформаційні війни. Уперше на науковому рівні це питання порушив відомий дослідник Е.Тоффлер, стверджуючи, що «для цивілізації третьої хвилі одним із головних видів сировини буде інформація» [9, с. 33]. Виходячи з того, що всі види ресурсів цивілізації поділяються на матеріальні й нематеріальні, інформаційну безпеку доцільно розглядати і досліджувати в двох вимірах: ***техніко-технологічному*** і ***гуманітарному***.

У ***техніко-технологічному вимірі*** методологічною базою для визначення вимог захисту інформаційних систем від несанкціонованого доступу, створення захисних систем та оцінювання ступеня захищеності є *критерії оцінки інформаційної безпеки*. Головним завданням таких стандартів інформаційної безпеки є узгодженість позицій і запитів трьох груп фахівців, які однаковою мірою їх використовують, – виробників, споживачів та експертів з кваліфікації рівня безпеки. Якщо для виробників першочергово важлива максимальна конкретність стандартів та загальні вимоги критеріїв, то для споживачів визначальними є простота критеріїв та однозначність параметрів вибору захищеної системи. Експерти ж використовують критерії для визначення відповідності між ІТ-продуктом і запропонованими до нього вимогами.

Початок вироблення стандартів інформаційної безпеки, на переконання переважної більшості дослідників, покладено у 1983 р. так званою «Оранжевою книгою» Міністерства оборони США – «Критерії оцінки надійних комп'ютерних систем». Згідно з цим документом безпечною є інформаційна система, яка керує доступом до даних, проте абсолютно безпечних систем не існує. Отже, доцільно оцінювати ступінь довіри до системи, її надійність. У 1986 р. країни Європи спільно розробили загальні

«Європейські критерії безпеки інформаційних технологій» [5, с. 390], якими, зокрема, визначені завдання засобів інформаційної безпеки. Для визначення ефективності та надійності засобів захисту в єврокритеріях було вперше введено поняття «адекватності засобів захисту» і визначено сім рівнів адекватності: за зростанням – від Е0 до Е6.

Якщо перший стандарт інформаційної безпеки – «Оранжева книга» – призначався для систем спеціального і військового споживання, то сфера застосування розроблених кількома роками пізніше єврокритеріїв значно розширена. До цього стандарту ввійшли: розподілені системи, мережі, системи телекомунікацій та системи управління базою даних. Розроблені в 1993 р. «Канадські критерії безпеки комп'ютерних систем» сферою свого застосування розглядають усі типи комп'ютерних систем. З метою створення єдиного міжнародного стандарту інформаційної безпеки спільними зусиллями авторів «Європейських критеріїв безпеки інформаційних технологій», «Федеральних критеріїв безпеки інформаційних технологій Росії» та «Канадських критеріїв безпеки комп'ютерних систем» у 1996 р. завершена робота з об'єднання цих стандартів в «Єдині критерії безпеки інформаційних технологій» (англ.: Common Criteria for Information Technology Security Evaluation), які проголошені невід'ємним компонентом інформаційних технологій.

Згідно з «Єдиними критеріями» для характеристики основних критеріїв інформаційної безпеки застосовується модель тріади CIA (англ.: CIA Triad), яка передбачає три основні характеристики інформаційної безпеки: конфіденційність, цілісність та доступність (англ. Confidentiality, Integrity and Availability (CIA)). Можливості несанкціонованого ознайомлення з інформацією вважаються загрозами *конфіденційності*. У разі, якщо існують вимоги до обмеження можливості модифікації інформації, їх відносять до критеріїв *цілісності*. Загрози, що належать до порушення можливості використання комп'ютерних систем або оброблюваної інформації, складають загрози *доступності*. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою є предметом спостережності й керованості. Інформаційні системи аналізуються в трьох головних секторах: технічних засобах, програмному забезпеченні та комунікаціях для ідентифікування і застосування промислових стандартів інформаційної безпеки як механізми захисту і запобігання на трьох рівнях: фізичному, особистому та організаційному.

«Єдині критерії», на думку вітчизняних дослідників О.Петрова, О.Таликіна та А.Мініна [6, с. 92], дають змогу за допомогою механізмів профілів захисту: споживачам – створювати приватні комплекси вимог, що відповідають їхнім потребам; розробникам – використовувати як основу для створення специфікацій своїх продуктів. Профіль захисту і сертифікації засобів захисту складають Проект захисту, що подає ІТ-продукт у процесі кваліфікаційного аналізу. За допомогою профілів захисту споживачі формулюють свої вимоги до виробників. Проект захисту містить вимоги і завдання захисту ІТ-продукту, а також описує рівень функціональних можливостей реалізованих у ньому засобів захисту, їхнє обґрунтування і підтвердження ступеня їхньої адекватності, отже являє собою основу для спільної роботи виробників і експертів з кваліфікації. На переконання науковців, головні переваги «Єдиних критеріїв» – повнота вимог інформаційної безпеки, гнучкість у застосуванні й відкритість для подальшого розвитку з урахуванням новітніх досягнень науки й техніки.

Найбільш вдалим, на наш погляд, визначенням техніко-технологічного виміру інформаційної безпеки та захисту інформації є «захищеність інформації і підтримуючої інфраструктури від випадкових та навмисних впливів природного та штучного характеру, у результаті яких наносяться збитки володарям або користувачам інформації і інфраструктурі, що їх підтримує [4, с. 13]. Інформаційна безпека забезпечується за рахунок захисту інформації». У свою чергу, захистом інформації є комплекс заходів, спрямованих на забезпечення необхідного рівня *інформаційної безпеки*.

Сучасний рівень розвитку цивілізації, на переконання відомого вітчизняного науковця Г.Почепцова, є причиною того, що «інформація несе у собі як творчу, так і руйнівну силу, але набагато більшою мірою, аніж це було раніше» [7, с. 79]. Отже, поряд з безпекою інформаційних технологій та інформаційних ресурсів не менш важливим, на наш погляд, є ***гуманітарний вимір*** інформаційної безпеки, тобто захист від інформації та *інформаційна вразливість* особистості, суспільства, цивілізації. Використання нових прогресивних інформаційних технологій у суспільному житті, виробництві та управлінні, можливості швидкого обміну науково-технічною, економічною, навчальною та іншою інформацією є підтвердженням значущості інформації як системоутворювального соціального явища. Водночас суспільство, на думку українських дослідників, «з великим запізненням починає осмислювати політичні, економічні, соціальні, військові, психологічні та інші наслідки глобальної інформатизації» [4, с. 11]. Очевидно, що технологічно розвинені держави намагаються і продовжуватимуть збільшувати політичну, економічну та військову перевагу за рахунок досягнення переваг у рівні інформатизації; і, як наслідок, – установлення та проведення глобального інформаційного контролю над менш розвиненими державами,

проведення в загальному інформаційному просторі ідеологічної та культурної експансій.

Інформаційні війни велися постійно зі стародавніх часів і в більшості випадків справляли суттєвий вплив на становлення та розвиток різних держав. Проте саме терміни «інформаційна війна», «інформаційна операція» почали активно вживатися в 1991 р. після війни у Перській затоці. Яскравим та дієвим прикладом успішного ведення інформаційної війни, її впливу на кінцевий результат, на думку фахівців, була війна проти Іраку, що отримала назву «Буря в пустелі», де нові інформаційні технології вперше були застосовані у військових цілях. Першим офіційним документом з цього приводу, на думку науковців, була директива міністра оборони США № TS 3600.1 від 21 грудня 1992 р. «Інформаційна війна», результатом якої через рік стала директива Комітету начальників штабів Міністерства оборони США № 30-93, у якій інформаційну війну визначено як «комплексне проведення за єдиним задумом і планом психологічних операцій, заходів щодо оперативного маскування, радіоелектронної боротьби і фізичного знищення пунктів зв'язку з метою позбавлення супротивника інформації, виведення з ладу або знищення його систем управління при одночасному захисті своїх сил від аналогічних дій» [3, с. 41]. Цей документ, за оцінкою фахівців, став вихідною точкою для подальших як військових, так і державних документів та досліджень не тільки у США, а й в інших країнах світу [5, с. 425]. З 1994 р. у США проходять офіційні наукові конференції з питань інформаційних війн та створено Центр інформаційної стратегії і політики, головним завданням якого є вивчення можливостей використання інформаційних технологій у військових конфліктах XXI ст. У 1995 р. співробітники корпорації RAND провели військові ігри «Бій без поля бою – війна в XXI столітті» [1], у яких брали участь провідні фахівці США в галузі комп'ютерної безпеки з корпорацій, державних організацій та Міністерства оборони США. На цих іграх відпрацьовувалися питання вироблення стратегій захисту США у разі використання ворогом засобів інформаційної війни. Як потенційний ворог розглядався Іран. Надалі у всіх збройних конфліктах за участю США було задіяно різні види інформаційної зброї.

До ***інформаційної зброї,*** за визначенням вітчизняних науковців А.Чічановського та О.Старіша, належать спеціальні засоби, технології та дані, що допомагають впливати на інформаційний простір суспільства і завдавати збитків життєво важливим інтересам держави [5, с. 414]. Інформаційна зброя визначається комплексом засобів, призначених для:

– впливу на інформаційні системи супротивної сторони;

– упровадження в комп'ютерні мережі систем управління і телекомунікацій відповідних елементів і програмного забезпечення, що спотворюють дані;

– управління поведінкою людей шляхом впливу на їхню свідомість з допомогою системи засобів масової комунікації.

До сьогодні термін «інформаційна війна» має дискусійний та неоднозначний характер, зважаючи на те, що різні автори трактують його порізному, залежно від того, які аспекти проявів та змісту вони досліджують. Український науковець О.Дубас умовно поділяє дослідників інформаційних воєн на три основні групи [2, с. 69]: тих, хто віддає перевагу соціально-комунікативному підходу, розуміє інформаційну війну як окремі інформаційні заходи, інформаційні способи та засоби корпоративної конкуренції, ведення міждержавного протиборства, збройної боротьби, комунікаційні технології впливу на масову свідомість. До другої групи дослідників входять, в основному, представники військових відомств, які відносять інформаційну війну до сфери військового протиборства й розглядають її як комплексне спільне застосування сил і засобів інформаційної та збройної боротьби (військово-прикладний підхід). На думку третьої групи вчених, інформаційна війна – це явище мирного періоду міждержавного протиборства, яке дає змогу вирішувати зовнішньополітичні завдання несиловим у традиційному розумінні методом.

На переконання українських дослідників І.Горбатенка, В.Долгова, Т.Гріненко, інформаційна війна є протиборством непримиренних сторін у відповідному інформаційному просторі, яке здійснюється з використанням інформаційної зброї з метою нанесення максимальних витрат «супротивнику» та мінімізації особистих витрат в економічній, військовій, політичній, ідеологічній як у цілому, так і в окремих сферах [4, с. 11].

Один з перших теоретиків інформаційних протиборств Мартін Лібікі визначає сім форм інформаційної війни [5, с. 408]:

– боротьба із системою управління і комунікацій супротивника;

– боротьба за інформацію про власні сили і сили супротивника для отримання вирішальної переваги над супротивником;

– радіоелектронна боротьба;

– боротьба з гуманітарними системами супротивника;

– боротьба з техніко-технологічними системами супротивника;

– блокування чи спрямування даних про економічний стан у потрібне русло задля економічного домінування.

Зауважуючи, що єдиним компонентом, присутнім упродовж усіх етапів інформаційної війни, є боротьба з гуманітарними системами супротивника, тобто ***психологічна війна***, науковець диферецює психологічну війну на окремі сегменти, а саме:

– операції проти національної самосвідомості;

– операції проти керівництва супротивної сторони;

– операції проти військ супротивника;

– культурні конфлікти.

При цьому він зазначає, що сторона, яка збирається маніпулювати іншою за допомогою засобів масової комунікації, найперше має визначити цільові аудиторії супротивної сторони. Найважливіше завдання на підготовчому етапі інформаційного протиборства, на думку аналітиків, є використання можливостей засобів масової комунікації задля: введення в оману потенційного супротивника, дискредитації його військово-політичного керівництва та лідерів, обмеження інформаційно-пропагандистської діяльності супротивника аж до організації інформаційної блокади.

Безумовно, що намагаючись отримати перевагу в різних сферах, технологічно розвинені держави будуть намагатися впливати на інші держави. Так, «боротьба культур», на думку М.Лібікі, не будучи формою озброєного протиборства, ставить своїм завданням культурну експансію, яка також полегшує застосування психологічної зброї і, що найголовніше, дає змогу точніше спрогнозувати результати цього застосування. Ще однією рисою конфліктів нового покоління стало прагнення до інтелектуального домінування, на відміну від фізичного домінування в минулому. Бажання перемогти супротивника не воюючи чи позбавити його можливості чинити опір призвело до ще однієї форми інформаційної війни – економічного домінування. Об'єднання методів інформаційної й економічної війн, на думку науковця, зумовлює такі форми протиборства, як блокування відомостей про економічну потужність та інформаційний імперіалізм, який полегшує транснаціональним корпораціям, що втратили національні ознаки, боротьбу за економічне домінування.

За допомогою комплексного підходу вітчизняним дослідником А.Фісуном здійснено спробу вивести синтетичне поняття: ***інформаційна війна*** – це комплексний відкритий чи прихований цілеспрямований інформаційний вплив однієї сторони, чи взаємний вплив сторін одна на одну, який охоплює систему методів та засобів впливу на людей, їхню психіку та поведінку, на інформаційні ресурси та інформаційні системи з метою досягнення інформаційної переваги в забезпеченні національної стратегії, здатної привести до прийняття сприятливих для ініціатора впливу рішень або паралізувати інформаційну інфраструктуру супротивника з одночасним зміцненням і власним захистом інформації та інформаційних систем [10, с. 46]. Інформаційна війна припускає порушення, ушкодження, модифікацію інформаційних ресурсів і знань людей про самих себе та навколишній світ і впливає на суспільну думку та думку еліт, заходи дипломатичного характеру, пропагандистські та психологічні кампанії, підривні акції в галузі культури й політики, дезінформацію та впровадження в місцеві медіа-канали, проникнення в комп'ютерні мережі й бази даних, технічне сприяння дисидентським і опозиційним рухам і надання їм інформаційної підтримки.

З розвитком технічних засобів, на переконання українського науковця О.Дубаса, збільшується число прийомів ведення інформаційної війни: від «інформаційної боротьби першого покоління», що розглядалася її авторами як розширення класичної радіоелектронної боротьби, до «інформаційної боротьби третього покоління», під якою розуміються операції на основі ефектів [2, с. 71]. Саме операції на основі ефектів сьогодні є основою реалізації зовнішньої політики розвинених держав в інформаційну епоху. Основоположним аспектом інформаційного протиборства було і залишається прагнення до інформаційної переваги.

Висновки до пропонованого дослідження та перспективи подальших розвідок у цьому напрямі. Теоретико-методологічний аналіз міжнародних критеріїв інформаційної безпеки дає змогу виділити два основні підходи до дослідження цих критеріїв. У рамках першого підходу розглядається техніко-технологічний вимір інформаційної безпеки. Інформаційна війна розуміється як протиборство інформаційно-комунікаційних технологій та здатності державних і комерційних інформаційних систем забезпечити безпеку інфраструктури держави в цілому. До техніко-технологічного виміру, на наш погляд, варто віднести такі міжнародні критерії інформаційної безпеки:

– захист інформаційних ресурсів від несанкціонованого доступу з метою забезпечення конфіденційності;

– забезпечення цілісності інформаційних ресурсів шляхом їх захисту від несанкціонованої модифікації або знищення;

– забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні.

Другий підхід виходить із гуманітарного виміру інформаційної безпеки та опису явища інформаційної війни через її вплив на масову свідомість, маніпулятивний потенціал і психологічний вплив інформаційних повідомлень. До міжнародних критеріїв інформаційної безпеки гуманітарного виміру, зокрема, належить:

– захист власної інформації та інформаційних систем;

– протидія негативному впливу на людську свідомість з допомогою системи засобів масової комунікації;

– захист інформаційних ресурсів і знань людей про самих себе та навколишній світ;

– протидія пропагандистським та психологічним кампаніям, підривним акціям у галузі культури і політики.

В умовах інформаційної війни об'єктами руйнування стають ціннісні орієнтири суспільства, національний менталітет, суспільний ідеал, а одним з основних інструментів деструктивного інформаційного впливу стають засоби масової комунікації. Отже, проблема гарантування інформаційної безпеки особистості й суспільства має комплексний характер і для її розв'язання потрібне системне об'єднання на державному рівні законодавчих, організаційних та програмно-технічних засобів.

Темою подальших досліджень у розглянутій сфері може стати аналіз інформаційних загроз і вироблення адекватних заходів їх протидії, визначення основних критеріїв захисту вітчизняних інформаційних систем та формування державної політики інформаційної безпеки. Усвідомлення існуючих і прогнозування потенційних проблем у сфері інформаційної безпеки вимагають постійного вдосконалення критеріїв і технологій інформаційної безпеки, що перебуває в постійній динамічній корекції законодавчих актів і технічних засобів.

Список використаних джерел

1. Бой без поля боя – война в 21 веке [Электронный ресурс] / (По материалам корпорации RAND). – Режим доступа : http://www.wplus.net/~kvn/gensec.htm
2. *Гриценко О. М.* Українські ЗМІ в контексті глобальних процесів на початку XXI століття / О. М. Гриценко // Україна на шляху до Європи / упоряд. : В. І. Шкляр, А. В. Юричко. – К. : Етнос, 2006. – С. 265–379.
3. *Дубас О. П.* Інформаційна війна: нові можливості політичного протиборства / О. П. Дубас // Освіта регіону. – 2010. – № 1. – С. 69–72.
4. *Жуков В.* Взгляды военного руководства США на ведение информационной войны / В. Жуков // Зарубежное военное обозрение. – 2001. – № 1.
5. *Горбенко І. Д.* Інформаційна війна – сутність, методи та засоби ведення / І. Д. Горбенко, В. І. Долгов, Т. О. Гріненко : матеріали ювіл. наук.-техніч. конф. – К., 1998. – С. 11–14.
6. *Чічановський А. А.* Інформаційні процеси в структурі світових комунікаційних систем : підручник / А. А. Чічановський, О. Г. Старіш. – К. : Грамота, 2010. – 568 с.
7. *Петров О. С.* Критерії оцінки захищеності інформації в комп'ютерних системах: поєднання єдиних критеріїв та критеріїв України / О. С. Петров, О. А. Таликін, А. В. Мінін // Вісн. Східноукр. нац. ун-ту ім. В. Даля. – 2005. – № 1.
8. *Почепцов Г. Г.* Информационные войны / Г. Г. Почепцов. – К. : Ваклер, 2000.
9. *Расторгуев С. П.* Информационная война / С. П. Расторгуев. – М. : Радио и связь, 1999.
10. *Рубан В. Я.* Інформаційна безпека України: сутність та проблеми / В. Я. Рубан // Стратегічна панорама. – 1998. – № 3–4. – С. 12.
11. *Тоффлер Э.* На пороге будущего / Э. Тоффлер // «Американская модель»: с будущим в конфликте. – М., 1984.
12. *Фісун А. О.* Теоретично-категоріальне осмислення поняття «інформаційна війна» в структурі інформаційно-політичного простору / А. О. Фісун // Інформаційне суспільство. – 2011. – Вип. 13. – С. 43–48.

References

1. Boy bez polya boya – voyna v 21 veke [Fighting the battle – the war in the 21st century]. / (Po materialam korporatsii RAND). – Rezhim dostupu: http://www.wplus.net/~kvn/gensec.htm
2. Gritsenko O. M. UkraYinskI ZMI v kontekstI globalnih protsesIv na pochatku HHI stolIttya [Ukrainian media in the context of global processes in the early twenty-first century] / UkraYina na shlyahu do Evropi: Nauk. vid. / Uporyad.: V. I. Shklyar, A. V. Yurichko. – K.: Etnos, 2006. – S. 265-379.
3. Dubas O.P. Informatsiyna viyna: novi mozhlivosti politichnogo protiborstva [Information warfare: new opportunities for political confrontation] / Ukrainskiy naukoviy jurnal " Osvita regionu ." / K. : 2010 - № 1. - S. 69-72
4. Zhukov V. Vzglyadyi voennogo rukovodstva SShA na vedenie informatsionnoy voynyi [Views of the U.S. military leadership to conduct information warfare] / Zarubezhnoe voennoe obozrenie - # 1. – 2001.
5. Informatsiyna viyna - sutnist, metody ta zasoby vedennya [Information warfare - the nature, methods and means of]. / Gorbenko I. D., Dolgov V. I., Grinenko T.S. Materiali yuvileynoi naukovyi- tehnichnoi konferentsii . / K. : - 1998. - S. 11-14 .
6. Informatsiyni protsesi v strukturi svitovih komunikatsiynih sistem: Pidruchnik [Information processes in the structure of global communication systems: Tutorial]. / A. A. Chichanovskiy, O. G. Starish. – K.: Gramota, 2010. – 568 s.
7. Kriteriyi otsInki zahischenosti Informatsiyi v komp'yuternih sistemah: poednannya edinih kriteriyiv ta kriteriyiv Ukrayini [Criteria for evaluating the security of information in computer systems: a combination of uniform criteria and criteria Ukraine]. / Petrov O.S., Talikin O.A., Minin A.V. – Visnik Shidnoukrayinskogo natsionalnogo universitetu im. V. Dalya, 2005.
8. Pocheptsov G.G. Informatsionnyie voynyi [Information warfare]. – K.: Vakler, 2000.
9. Rastorguev S.P. Informatsionnaya voyna [Information warfare]. – M.: Radio i svyaz, 1999.
10. Ruban V. Ya. InformatsIyna bezpeka UkraYini: sutnIst ta problemi [Securing Ukraine: the nature and problems] / StrategIchna panorama # 3-4, 1998. – S. 12
11. Toffler E. Na poroge buduschego [On the threshold of the future]. / «Amerikanskaya model»: s buduschim v konflikte. – M., 1984.
12. Fisun A.O. Teoretichno-kategorialne osmislennya ponyattya «Informatsiyna viyna» v strukturi informatsiyno-politichnogo prostoru [Theoretical and categorical understanding of the concept of «nformation war» in the structure of information and political space]. / «InformatsIyne suspilstvo». – Vipusk 13, sIchen-cherven, 2011 r. – s. 43-48