УДК 65.012.8:007+32(477)

Боднар І. Р., Вовчанська О. М.

ДЕРЖАВНА ПОЛІТИКА ТА ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ: ПІСЛЯКРИЗОВІ ВИКЛИКИ

Анотація. *Розглянуто основні напрями державної інформаційної політики. Аналізуються інформаційні загрози національній безпеці України та шляхи гарантування інформаційної безпеки. Запропоновані підходи щодо забезпечення процесу безперервності функціонування системи інформаційної безпеки держави.*

Ключові слова: державна політика, інформаційна безпека, інформаційні загрози, інформаційні ресурси, національна безпека.

I. Bodnar., O.Vovchanska

STATE POLICY AND INFORMATION SECURITY OF UKRAINE: POST-CRISIS CHALLENGES

Abstract. *The main directions of state information policy are considered. The information threats analysis for national security of Ukraine and ways of ensuring of information security are analyzed. The approaches for the process continuity of functioning of the system of information security are proposed.*

Keywords: state policy, information security, information threats, information resources, national security.

1. Вступ

Інформаційна безпека у сучасному постіндустріальному світі, в якому постійно виникають кризи, конфлікти, є основою національної безпеки країни. Проведення ефективної державної інформаційної політики позитивно впливає на вихід із внутрішньополітичних та зовнішньополітичних криз і вирішення конфліктів. Вперше проблема інформаційної безпеки була відзначена США ще в 1947 р. У країні був прийнятий закон "Про національну безпеку". У 2012 р. експерти США визначили основну кібер-загрозу національній безпеці країни на наступне десятиліття.

Інформаційна безпека розглядається як глобальна проблема захисту інформації, інформаційного національного простору, суверенітету країни та інформаційного забезпечення прийняття урядових рішень. Захищаючи свої інформаційні інтереси, кожна держава повинна дбати про свою інформаційну безпеку. Цього ж вимагає і зміцнення української державності. Збалансована державна інформаційна політика України формується як складова частина її соціально-економічної політики, виходячи з пріоритетності національних інтересів та загроз національній безпеці країни.

Захист інформаційної сфери є основою наукових досліджень вітчизняних та зарубіжних вчених. Вивченням ролі держави у формуванні інформаційного суспільства та забезпеченні інформаційної безпеки займаються такі вчені, як Г. Почепцов [1], І. Рамоне [2], О. Соснін [3] І. Арістова [4] та ін.

Мета статті полягає у необхідності теоретичного обґрунтування основних напрямів державної інформаційної політики з метою захисту національного інформаційного простору та гарантування інформаційної безпеки в посткризовий період.

2. Державна політика забезпечення інформаційної безпеки

В Україні всі види інформаційних технологій, їхнього виробництва та засоби забезпечення цих технологій становлять спеціальну сферу діяльності, розвиток якої визначається державною інформаційною політикою та Національною програмою інформатизації. Визначення завдань Національної програми інформатизації, пріоритетних напрямів розвитку інформатизації, обсягів, джерел і порядку їх бюджетного фінансування покладається на Кабінет Міністрів України і щорічно затверджується Верховною Радою України.

Національну безпеку України в інформаційній сфері слід розглядати як інтегральну цілісність чотирьох складових: персональної, публічної (суспільної), комерційної (корпоративної) й державної безпеки. Тому в процесі визначення характеру ризиків слід брати до уваги наступні елементи:

- концептуальні засади політичної безпеки, її принципи, стандарти та правила, погоджені з чинним законодавством та принципами забезпечення безперервності системи інформаційної безпеки особистості, суспільства, комерційних (корпоративних) структур та держави;
- визначення об'єктів та цілей;
- визначення прийнятних з погляду забезпечення інтересів усіх суб'єктів структур встановлення контролю над об'єктами безпеки, а також оцінка ризиків та управління ними;
- визначення статусно-функціональних ролей, очікувань та міри відповідальності суб'єктів включно

зі звітністю про події, які пов'язані з потенційними загрозами [5].

Розрізняють такі цілі державної політики гарантування інформаційної безпеки:

1. Реалізація конституційних прав громадян, суспільства та держави на інформацію.

2. Захист інформаційного суверенітету країни, зокрема національного інформаційного ресурсу, систем формування суспільної свідомості.

3. Забезпечення рівня інформаційної достатності для прийняття рішень державним установам, підприємствам та громадянам.

4. Належна присутність країни у світовому інформаційному просторі.

До завдань політики гарантування інформаційної безпеки належать:

1. Виявлення, оцінка та прогнозування поведінки джерел загроз інфор-маційній безпеці, що здійснюються шляхом оперативного моніторингу інформаційної ситуації.

2. Вироблення, координація та введення єдиної державної політики у галузі інформаційної безпеки.

3. Створення та експлуатація систем гарантування інформаційної безпеки.

4. Розробка, координація та запровадження єдиної державної політики у сфері міжнародних інформаційних відносин, зокрема у напрямі формування іміджу держави.

На особливу увагу заслуговує проблема забезпечення конституційних прав громадян на інформацію. Але розвиток інформаційних технологій пов'язаний як із позитивними, так і негативними сторонами. Вдосконалення засобів обробки і передачі інформації створює умови для розквіту демократичних суспільств, участі громадян у прийнятті найважливіших рішень тощо.

Враховуючи цілі та завдання політики інформаційної безпеки, виокремимо чотири основні напрями її забезпечення:

1. Забезпечення інформаційної достатності для прийняття рішень.

2. Захист інформації (інформаційних ресурсів).

3. Захист та контроль національного інформаційного простору, тобто систем формування масової свідомості.

4. Присутність у світовому інформаційному просторі.

Однією з найважливіших умов якісного інформаційного забезпечення є наявність багатьох інформаційних джерел. Це зменшує можливість дезінформації, проте необхідна рівновага між ними. Важливим напрямом забезпечення інформаційної достатності є визначення надійності джерел інформації. Підходи до тлумачення фактів значною мірою визначаються системою настанов, стереотипів та символів аналітика, тому не виключені можливості цілеспрямованих пропагандистських кампаній проти аналітиків, осіб, що приймають рішення. На сучасному етапі визначальними у прийнятті політичних та економічних рішень є аналіз зібраної інформації, тобто виокремлення так званих "шумів" і правильна інтерпретація інформації.

Доступність та якість інформаційного забезпечення визначають темпи науково-технічного та економічного розвитку країни.

У загальній системі захисту інформації вирізняються такі напрями:

- законодавчо-нормативне забезпечення – передбачає розробку відповідних законодавчих актів, нагляд за виконанням законодавства з боку правоохоронних органів, судовий захист;

- організаційно-технічне забезпечення – розкриває систему заходів, спрямованих на недопущення реалізації загроз безпеці інформаційного ресурсу;

- страхування інформаційних ризиків – прийнятне лише для недержавних установ.

З метою забезпечення надійного захисту інформації в інформаційних системах вимоги безпеки необхідно враховувати вже під час їхнього проектування.

Надійне гарантування безпеки інформації у будь-якій інформаційній системі потребує системного підходу, побудови комплексної системи захисту (рис. 1).

Питання гарантування національної інформаційної безпеки розглядається на одному рівні із захистом суверенітету і територіальної цілісності країни. Концепція інформаційної безпеки України спрямована на визначення методів та засобів захисту інформації, створення засад формування державної політики, розвитку інформаційного простору країни, вироблення та реалізацію державної політики в сфері міжнародних інформаційних відносин.

Державна політика забезпечення інформаційної безпеки країни визначає основні напрями діяльності органів державної влади в інформаційній сфері. Ці напрями обумовлені змістом національних інтересів держави, суспільства та особистості. Основою гарантування інформаційної безпеки є мінімізація шкоди через неповноту, несвоєчасність або недостовірність інформації чи негативного інформаційного впливу через наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації. Саме тому інформаційна безпека передбачає наявність певних державних інститутів і умов існування її суб'єктів, що встановлені міжнародним і вітчизняним законодавством.

Якщо заподіюється шкода в результаті недосконалості інформаційних відносин, використання неякісної інформації тощо, це свідчить про зниження інформаційної безпеки [6]. Таке визначення дає змогу розглядати як невирішені проблеми гарантування інформаційної безпеки в Україні наступне:

- недосконаліть інформаційної політики та політики інформаційної безпеки держави;

- недосконаліть нормативно-правової бази в сфері інформаційних відносин та інформаційної безпеки;

- недостатню розвиненість інформаційної інфраструктури держави;

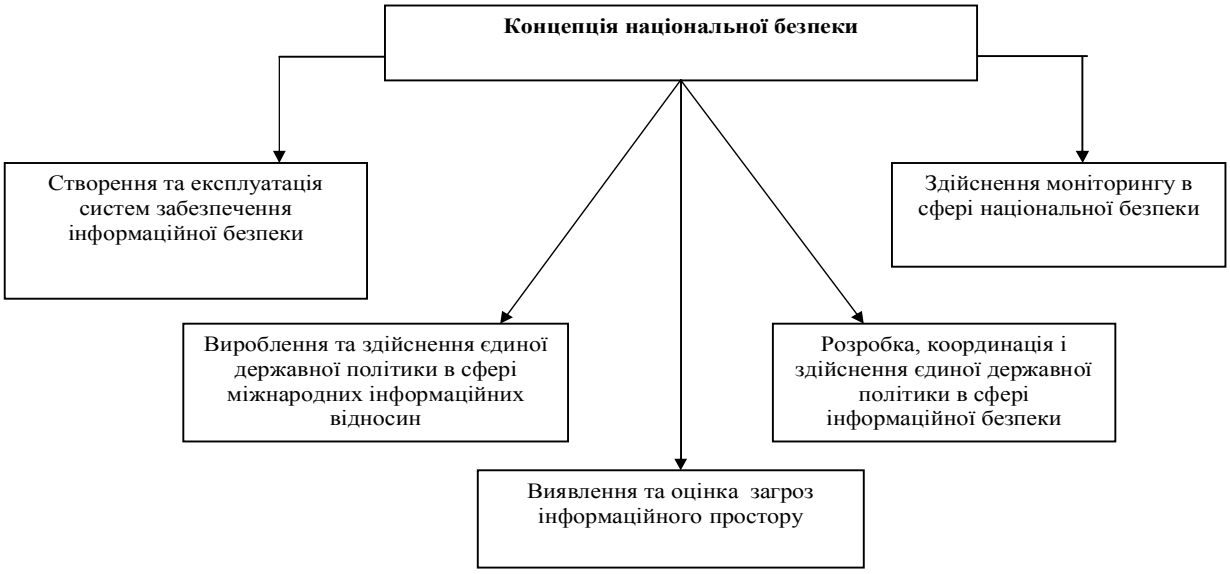


Рис. 1. Основні концепції національної безпеки
[Розроблено автором]

- введення іноземними державами обмежень по відношенню до України щодо розповсюдження інформації та отримання нових інформаційних технологій;
- протиправна діяльність посадових осіб, різних формувань та груп у сфері інформаційних інтересів громадян та держави;
- недосконаліть державної системи забезпечення інформаційної безпеки;
- можливість виникнення нештатних, непередбачених ситуацій у системах, процесах, що базуються на використанні інформаційних технологій тощо.

3. Законодавчі норми щодо гарантування інформаційної безпеки

Інформаційна безпека є однією з суттєвих складових частин національної безпеки країни. Її забезпечення завдяки послідовній реалізації національної інформаційної стратегії значною мірою сприяло би забезпеченню досягнення успіху при вирішенні завдань у політичній, соціальній, економічній та інших сферах державної діяльності. Проведення вдалої інформаційної політики може суттєво вплинути на вирішення внутрішньополітичних, зовнішньополітичних та військових конфліктів. У ст. 17 Конституції України зазначено: "Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу" [5]. Інформаційну безпеку слід розуміти як сукупність засобів забезпечення інформаційного суверенітету України, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз. Ця безпека повинна включати ефективну протидію сукупності інформаційних загроз.

Втручання в інформаційні мережі розглядається як одна з найбільш ймовірних проблем національної безпеки. Інформаційні технології дають змогу країнам займати основні сектори на ринку високотехнологічних товарів. У 12-му п'ятирічному плані Китаю є зобов'язання виділити більше від 1 трлн. дол. на наукові дослідження, розробки та їх

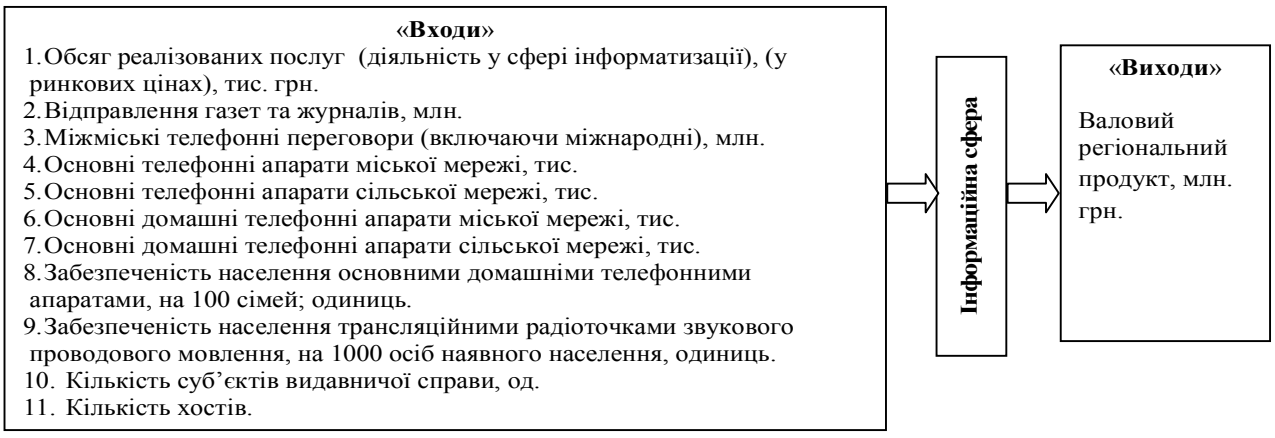


Рис. 2. Множина показників «входів» та «виходів» для оцінки ефективності використання інформаційних ресурсів України
[Розроблено автором]

впровадження у виробництво. Європа та Японія постійно демонструють новинки робототехніки, нанотехнологій.

Необхідність забезпечення інформаційної безпеки зумовлюється потребою забезпечення національних ресурсів [7]. Для визначення наявності та ефективності використання ресурсного потенціалу інформаційної сфери України було використано метод огортаючих даних, який дозволяє забезпечити співставність множини показників, які становлять інформаційний потенціал країни.

Результати дослідження ефективності використання ресурсів інформаційного комплексу за 11-ма показниками «входу» і одним показником «виходу» (валовий регіональний продукт, млн. грн.) (рис. 2) для областей України дозволили виділити дві групи регіонів за рівнем ефективності використання ресурсів (рис. 3): (1) регіони, які повною мірою використовують потенціал (коефіцієнт ефективності f =1); (2) регіони з низьким рівнем ефективності використання потенціалу (коефіцієнт ефективності f >1).

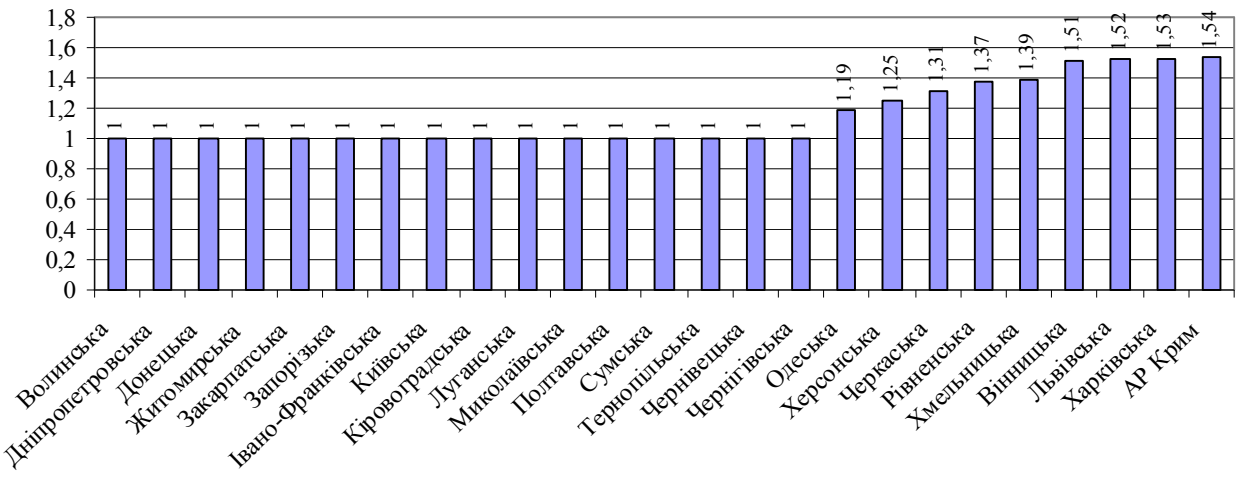
Як видно з рисунку 3, до регіонів із недостатньо ефективним використанням потенціалу інформаційних ресурсів відносяться Одеська (f=1,19), Херсонська (1,25), Черкаська (1,31), Рівненська (1,37), Хмельницька (1,39), Вінницька (1,51), Львівська (1,52), Харківська (1,53) області, АР Крим (1,54). Регіонам із показниками низької ефективності використання потенціалу інформаційної сфери доцільно змінити політику розвитку сфери та використання інформаційних ресурсів.

Забезпечення інформаційної безпеки зумовлюється також потребою забезпечення національної безпеки України в цілому. Завдання інформаційної безпеки – створення системи протидії інформаційним загрозам та захист власного інформаційного простору, інформаційної інфраструктури, інформаційних ресурсів держави. При виникненні криз, загострені конфліктів інформаційна боротьба може перерости в інформаційну війну, яка ведеться за допомогою інформаційної зброї. Показниками виступають цілеспрямованість, масштабність та комплексність дій тощо.

Зростання та ускладнення інформаційних атак вимагає нової державної інформаційної політики. Практичне вирішення проблем інформаційної безпеки, притягнення до відповідальності за порушення або загрозу інформаційній безпеці у кожній державі здійснюється у порядку, передбаченому нормами міжнародного права, відповідними міждержавними договорами, а також внутрішнім законодавством [9, 10]. Інформаційна безпека регулюється визначеними нормами міжнародного права, які зафіксовані у документах ООН і ЮНЕСКО, у документах європейських міжнародних організацій, а також у нормативних актах окремих держав. Так, існує міжнародна норма стосовно перекручення інформації, інформації, що підбурює до повалення державного ладу в тій чи іншій країні. В міжнародних документах зафіксований захист інтелектуальної інформації, а також захист комерційної інформації.

Кожна країна приймає закони про захист інформації в різних галузях. Франція прийняла закон "Про інформації, інформаційні файли та права людини" (1978 р.), Німеччина – закон "Про захист інформації" (1990 р.), Австрія, Бельгія, Данія, Ірландія – закон "Про захист інформації" (1991 р.), Фінляндія, Ісландія – закон "Про захист інформації про особу" (1994 р.), Люксембург – закон "Про використання інформації в процесі роботи з комп'ютером" (1993 р.). В Україні прийнятий закон "Про захист персональних даних" (2010 р.). Кожна країна встановлює закони для регулювання інформаційних потоків і захисту інформації, що становить державну таємницю. Такий перелік оновлюється кожного року відповідно до пріоритетів та інтересів держави.

В межах міжнародних організацій була прийнята Міжнародна конвенція "Про співробітництво та транскордонну передачу даних" (1982 р). У межах ЄС була прийнята Конвенція "Про захист персональної інформації у зв'язку з автоматизованою обробкою даних" (1991 р.). У 1998 р. за результатами 53-ої сесії ГА ООН розроблено резолюцію (A/RES/53/70) "Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки". Резолюція 53/70 поклала початок обговоренню створення абсолютно нового міжнародно-правового режиму, суб'єктами якого в перспективі повинні стати інформація та інформаційна технологія. У 1999 р. на 54-ій сесії ГА ООН було прийнято оновлений проект резолюції (A/RES/54/49) "Досягнення у сфері інформатизації і телекомунікацій в кон-



тексті міжнародної безпеки". Вперше було вказано на загрози міжнародній інформаційній безпеці відносно різних сфер економіки. За результатами роботи сесії було опубліковано проект "Принципів, що стосуються міжнародної інформаційної безпеки" (A/55/140У). Розроблено кодекс поведінки держав в інформаційному просторі, який передбачає відповідні моральні зобов'язання, а також закладає основи для широких міжнародних переговорів під егідою ООН та інших міжнародних організацій із проблем міжнародної інформаційної безпеки. У переліку принципів наводяться основні визначення понять: інформаційної безпеки, міжнародної інформаційної безпеки, загроз інформаційній безпеці, інформаційної зброї, інформаційної війни, міжнародного інформаційного тероризму. Базові принципи міжнародної інформаційної безпеки визначають роль і права, зобов'язання та відповідальність держав в інформаційному просторі, а також конкретні завдання, вирішення яких було б направлене на обмеження загроз у сфері МІБ, до того ж, прописують роль ООН в контексті загальних зусиль у цій сфері. За результатами роботи 55-ої сесії ГА ООН у 2000 р. схвалено новий проект резолюції (A/RES/55/28), в якому наголошується, що цілями обмеження загроз у сфері інформаційної безпеки є "вивчення відповідних міжнародних концепцій, спрямованих на зміцнення безпеки глобальних інформаційних і телекомунікаційних систем та реалізація їх пропозицій". Крім того, відповідно до рекомендацій резолюції 55/28 було підготовлено проект документа (A/56/164/Add.1) "Загальна оцінка проблем інформаційної безпеки. Загрози міжнародній інформаційній безпеці". В документі виділені та описані одинадцять основних чинників, що спричиняють небезпеку особи, суспільства і держави в інформаційному просторі, тобто є найбільшими загрозами міжнародній інформаційній безпеці. В 2004 р. створена спеціальна Група урядових експертів держав-членів ООН (ГУЕ) для проведення всестороннього дослідження проблеми міжнародної інформаційної безпеки. Прерогативою діяльності ГУЕ є розгляд існуючих і потенційних загроз у сфері інформаційної безпеки та сумісних заходів із їх усунення. В 2009 р. ООН прийняла програму "Розвиток ЗМІ і ЗМК та їх захист", в якому визначені міжнародні норми зміцнення безпеки глобальних інформаційних і телекомунікаційних систем.

4. Висновки

В Україні назріла об'єктивна потреба у державно-правовому регулюванні науково-технологічної та інформаційної діяльності, що відповідала б реаліям сучасного світу та рівню розвитку інформаційних технологій, нормам міжнародного права, але водночас ефективно захищала б власні українські національні інтереси. Відносини, пов'язані із забезпеченням інформаційної безпеки, як найважливіші сьогодні для суспільства та держави, вимагають найшвидшого законодавчого регулювання. Державна інформаційна політика повинна відображати нагальні питання, що склалися у міжнародній сфері та сфері інформаційної безпеки тощо. Необхідним є забезпечення законодавчого захисту прав та інтересів всіх суб'єктів інформаційних відносин. Найскладнішими тут є такі завдання, які передбачають гармонійне забезпечення інформаційної безпеки держави, особи і суспільства з одночасним виокремленням нагальних пріоритетів, до яких слід віднести створення/відновлення основних точок захисту системи національної безпеки в інформаційній сфері, перегляд списку нових інформаційних загроз, усунення наявних із визначенням ступеня можливих наслідків та рівнів їх інтенсивності. Основні акценти державної інформаційної політики повинні базуватися на забезпеченні права на достовірну, повну та своєчасну інформацію, свободи слова та інформаційної діяльності в національному інформаційному просторі, недопущення втручання в зміст та внутрішню організацію інформаційних процесів, крім випадків, визначених законодавством відповідно до Конституції України; збереженні та вдосконаленні вітчизняного національного інформаційного продукту та технологій, національно-духовних та культурних цінностей України; забезпеченні інформаційної та національно-культурної ідентифікації України у світовому інформаційному просторі; гарантуванні державної підтримки та розвитку ресурсів науково-технічної продукції та інформаційних технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Почепцов Г. Г. Інформаційна політика : навч. посібник / Г. Г. Почепцов. – К. : Знання, 2006. – 663 с.
2. Рамоне І. Глобальні трансформації та стратегії розвитку : монографія / І. Рамоне, Д. Лук'яненко. – К., 2010 – 453 с.
3. Соснін О. Державне управління інформатизацією як виклик цивілізаційного зростання нації / О. Соснін // Зовнішні справи. – 2011. – № 9. – С. 38-41.
4. Арістова І. В. Діяльність органів внутрішніх справ щодо реалізації державної інформаційної політики : монографія / І. В. Арістова. – Х. : Нац. ун-т внутр. справ, 2006. – 354 с.
5. Закон України. Про інформацію [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12.
6. Бондаренко В. О. Інформаційна безпека сучасної держави: концептуальні роздуми [Електронний ресурс]. – Режим доступу: www.crime-research.ru/library/strateg.html.
7. Супрун В. М. Інформаційний суверенітет як один з елементів інформаційної безпеки держави: теоретико-правовий аспект [Електронний ресурс]. – Режим доступу : http : // www.nbuv.gov.ua/portal/natural/vkhnu/Pravo/ 2009.
8. Веб-сторінка Державної служби статистики України [Електронний ресурс]. – Режим доступу : http : // www.ukrstat.gov.ua.
9. Ярочкін В. Система безпеки фірми [Електронний ресурс]. – Режим доступу : http : // www.nbuv.gov.ua.
10. Державна інформаційна політика [Електронний ресурс]. – Режим доступу : http : // merega.org.ua/law/projects/derzh polityka.