

УДК 316.774:351.75

Л. Євдоченко

## ШЛЯХИ ТА МЕТОДИ ДЕРЖАВНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ: ТЕОРЕТИЧНИЙ АСПЕКТ

Розглянуто теоретико-методологічні основи інформаційної безпеки України та її вплив на функціонування системи державного управління України, сутність та основні підходи до визначення національної безпеки, засоби її реалізації, шляхи забезпечення національної безпеки у сфері інформації в Україні, джерела загроз інформаційної безпеки України, методи забезпечення інформаційної безпеки України на сучасному етапі суспільного розвитку.

**Ключові слова:** національна безпека, інформаційна безпека, національні інтереси.

Сучасний етап розвитку суспільства характеризується зростаючою роллю інформаційної сфери, що є сукупністю інформації, інформаційної інфраструктури, суб'єктів, що здійснюють збір, формування, поширення й використання інформації, а також системи регулювання суспільних відносин, що виникають за цього. Інформаційна сфера є системоутворюючим чинником життя суспільства, активно впливає на стан політичної, економічної, оборонної й інших складових безпеки держави.

Стрімке зростання інформаційних технологій призвело до початку перерозподілу в суспільстві реальної влади від традиційних структур до центрів управління інформаційними потоками. Інформаційні технології знаходять усе ширше застосування у таких сферах, як фінансовий обіг і ринок цінних паперів, зв'язок, транспорт, високотехнологічні виробництва (особливо атомні, хімічні тощо), державні системи управління тощо. Будь-яка диверсія у наведених сферах життєдіяльності держави й суспільства може призвести до тяжких наслідків, паралізувати як ординарні, так і складні, “високі” системи управління, збройні сили і спеціальні служби, спровокувати руйнівні аварії на екологічнонебезпечних об'єктах.

Багато держав вкрай стурбовані станом інформаційної безпеки, залежність від якої зростатиме у ході технічного прогресу. Вони розробляють та впроваджують комплекс правових, організаційно-технічних та економічних заходів забезпечення інформаційної безпеки. Вихідними засадами таких заходів є доктрини, закони, концепції та інші нормативно-правові документи з інформаційної безпеки. Внаслідок цього розроблення та вдосконалення основ забезпечення інформаційної безпеки України є одним із найважливіших і особливо актуальних завдань держави.

Науковому осмисленню проблем реалізації інформаційної безпеки у сучасному постмодерному суспільстві сприяли праці сучасних дослідників: А. Даллеса О. Кастельса, В. Шапіро, Г. Веріана, К. Саркінеллі, С. Брауна, Й. Хабермаса, З. Аронсона, Д. Маклахана, К. Малaparте. Вони також розглядаються у працях Г. Авіцинової, М. Баглая, Е. Баталова, В. Левашова, П. Гончарова,

С. Рогачова, В. Жукова, Б. Краснова, Е. Тарасова. Особливий інтерес становить дослідження С. Кара-Мурзи.

В Україні вивчення цих питань розпочалося у 90-х рр. ХХ ст. Такі вчені, як Г. Почепцов, В. Королько, О. Голобуцький, В. Брижко, В. Цимбалюк, О. Олійник, О. Соснін, Л. Шиманський та інші. приділяють увагу вивченню особливостей становлення інформаційного суспільства в українських реаліях, визначають основні завдання і напрями державної інформаційної політики та можливі загрози національній безпеці. Однак на сьогодні питання вироблення сучасної моделі державного управління інформаційною сферою залишається відкритим і потребує подальших досліджень.

Задекларована нами проблематика виступала предметом спеціального розгляду у працях таких вітчизняних та зарубіжних вчених, як: Г. Нісевич, Н. Нижник, С. Чукут, Г. Почепцов, О. Литвиненко, В. Князев. Враховуючи те, що ця проблематика має ґрунтовну теоретико-методологічну базу дослідження, ми мали певні складнощі щодо розробки оптимальної структури розгляду, а тому намагались дослідити саме ті аспекти, які становлять фундаментальний соціальний та теоретико-практичний інтерес для її вирішення.

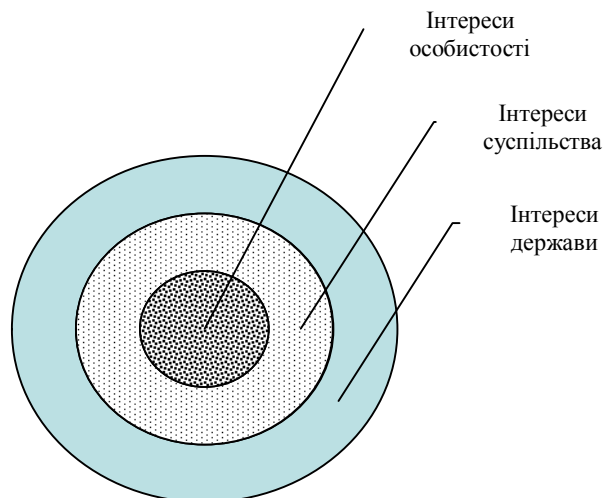
Метою статті є науково-теоретичний аналіз складових державного забезпечення інформаційної безпеки в Україні: з'ясування сутності складових національної безпеки; систематизація основних загроз та визначення їх джерел; аналіз засобів і методів організації їх протидії; аналіз особливостей функціонування та розробка шляхів реалізації державної політики у сфері інформаційної безпеки.

Доцільно зауважити, що в Україні саме поняття “інформаційна безпека” законодавчо не визначено [1]. Однак існуючі наукові та практичні підходи до вказаної проблеми дозволяють зробити висновок, що під інформаційною безпекою (особи, суспільства, держави) називають такий стан їхньої інформаційної озброєності (технічної, інтелектуальної, морально-етичної, політичної), за якого зовнішні інформаційні впливи не мають вирішального значення при прийнятті рішень, спрямованих на забезпечення власних (особистих, суспільних, державних) інтересів. За цього основним критерієм ефективності системи забезпечення інформаційної безпеки є зведення до мінімуму завдання шкоди через неповноту, невчасність і недостовірність інформації, а також через несанкціоноване поширення або отримання інформації.

Окрім того, розглядаючи інформаційну безпеку як складову національної безпеки, потрібно враховувати, що будь-яка із складових національної безпеки (політична, економічна, військова тощо) також містить у собі інформаційну компоненту (продаж озброєнь, наприклад, є можливим лише за умови відповідного рекламного-інформаційного забезпечення). А отже, інформаційна складова притаманна практично всім існуючим суспільним відносинам, що унеможливорює повний аналіз законодавства з інформаційної безпеки як такий.

З огляду на зазначене, найважливішими аспектами інформаційної безпеки є загальні питання розповсюдження і доступу до інформації у суспільстві та захист інформації з обмеженим доступом.

У контексті окресленої проблематики поняття інформаційної безпеки України трактуємо як стан захищеності її національних інтересів у інформаційній сфері, що визначаються сукупністю збалансованих інтересів особистості, суспільства й держави.



**Рис. 1. Збалансованість національних інтересів в інформаційній сфері.**  
**Інтереси держави**

Кожна із цих складових, зображених на рис. 1, має свої особливості, які торкаються наступних сфер:

- особистості – реалізації конституційних прав особи й громадянина на доступ до інформації, на використання інформації в інтересах здійснення діяльності, яка не заборонена законом, фізичного, духовного й інтелектуального розвитку, а також у захисті інформації, що забезпечує особисту безпеку;

- суспільства – забезпеченні інтересів особистості в цій сфері, зміцненні демократії, створенні правової соціальної держави, досягненні і підтримці суспільної злагоди, у духовному відновленні України;

- держави – у створенні умов для гармонічного розвитку інформаційної інфраструктури України з метою забезпечення непорушності конституційного ладу, суверенітету і територіальної цілісності України, політичної, економічної і соціальної стабільності, у безумовному забезпеченні законності і правопорядку, розвитку рівноправного й взаємовигідного міжнародного співробітництва [2].

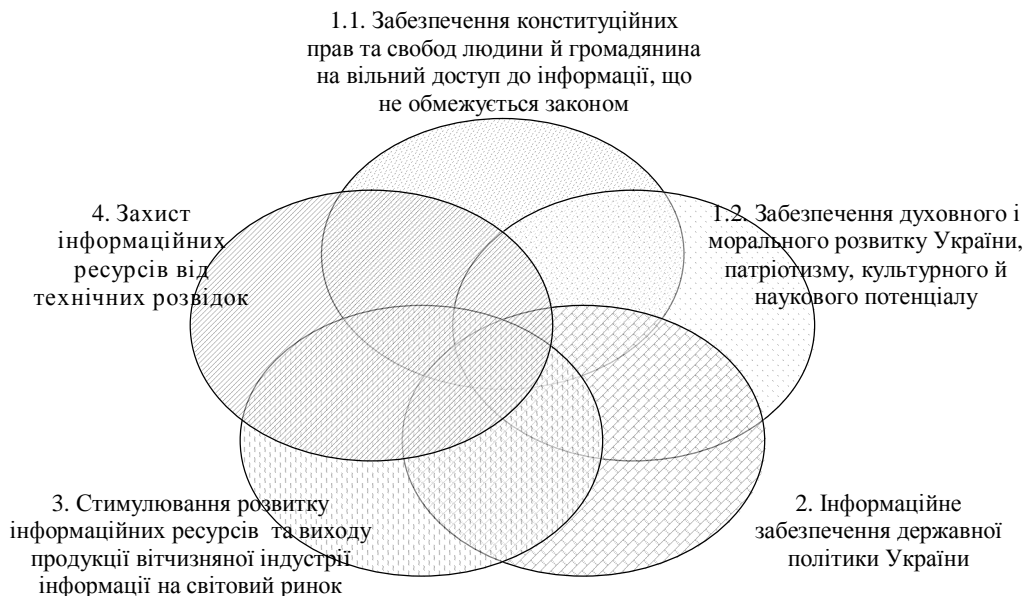
На основі національних інтересів України в інформаційній сфері формуються стратегічні й поточні завдання внутрішньої та зовнішньої політики держави із забезпечення інформаційної безпеки (рис. 2).

Перша складова національних інтересів України в інформаційній сфері (рис. 2) спонукає державу забезпечити конституційні права та свободи людини й громадянина вільно шукати, одержувати, передавати, робити й поширювати інформацію будь-яким законним способом, одержувати достовірну інформацію про стан навколишнього середовища, гарантувати свободу масової інформації й заборону цензури. Але держава також повинна зміцнювати механізми правового регулювання відносин у галузі охорони інтелектуальної власності, створити умови для дотримання установлених законодавством обмежень на доступ до інформації, яка не підлягає поширенню [3]:

- не допускати пропаганду й агітацію, що сприяють розпаленню соціальної, расової, національної чи релігійної ненависті і ворожнечі;

– забезпечити заборону на збирання, зберігання, використання й поширення інформації про приватне життя особи без її згоди та іншої інформації, доступ до якої обмежено законодавством;

– здійснювати захист особистої та сімейної таємниці, таємниці листування, телефонних переговорів, поштових, телеграфних та інших повідомлень, захист честі і свого доброго імені особи, а також захист комерційної таємниці [4].



**Рис. 2. Стратегічні й поточні завдання внутрішньої та зовнішньої політики України із забезпечення інформаційної безпеки**

Вагомим фактором першої складової національних інтересів в інформаційній сфері є державне забезпечення духовного відновлення України, збереження й зміцнення моральних цінностей суспільства, традицій патріотизму, гуманізму, культурного й наукового потенціалу країни.

Друга складова національних інтересів полягає у доведенні до її громадян та міжнародної громадськості достовірної інформації про державну політику України, її офіційної позиції щодо соціально значимих подій у житті держави і міжнародного життя, із забезпеченням доступу громадян до відкритих державних інформаційних ресурсів. Для цього потрібно: зміцнювати державні засоби масової інформації, розширювати їх можливості щодо своєчасного доведення достовірної інформації до громадян України та іноземних громадян; прискорити формування відкритих державних інформаційних ресурсів, підвищити ефективність їх використання. Вагоме значення має цілеспрямована робота в напрямку збільшення вітчизняного сегменту в світовому інформаційному просторі і формування в ньому позитивного іміджу України [5].

Третя складова національних інтересів України в інформаційній сфері полягає у розвитку сучасних інформаційних технологій, вітчизняної індустрії інформації, зокрема індустрії засобів інформатизації, телекомунікації та зв'язку, забезпеченні

потреб внутрішнього ринку її продукцією та вихід цієї продукції на світовий ринок, а також забезпеченні накопичення, зберігання та ефективного використання вітчизняних інформаційних ресурсів. У сучасних умовах тільки на цій основі можна вирішувати проблеми створення наукоємних технологій, технологічного переозброєння промисловості, збільшення досягнень вітчизняної науки й техніки. Держава повинна зайняти гідне місце серед світових лідерів мікроелектронної й комп'ютерної промисловості. Для цього потрібно:

- розвивати й удосконалювати інфраструктуру єдиного інформаційного простору України;
- розвивати вітчизняну індустрію інформаційних послуг і підвищувати ефективність використання державних інформаційних ресурсів;
- розвивати виробництво в Україні конкурентноспроможних засобів і систем інформатизації, телекомунікації та зв'язку, розширювати участь України в міжнародній кооперації виробників таких засобів і систем;
- забезпечити державну підтримку вітчизняних фундаментальних і прикладних досліджень, розробок у сферах інформатизації, телекомунікації та зв'язку.

Четверта складова національних інтересів України в інформаційній сфері полягає у захисті інформаційних ресурсів від технічних розвідок, несанкціонованого доступу, забезпеченні безпеки інформаційних і телекомунікаційних систем. Для цього потрібно:

- забезпечити ефективну протидію технічним розвідкам;
- підвищити безпеку інформаційних систем, включаючи мережі зв'язку, насамперед безпеку первинних мереж зв'язку та інформаційних систем органів державної влади, фінансово-кредитної та банківської сфер, сфери господарської діяльності, а також систем і засобів інформатизації озброєння і військової техніки, систем керування військами та зброєю, екологічно небезпечними й економічно важливими виробництвами;
- прискорити розвиток вітчизняного виробництва апаратних і програмних засобів захисту інформації та методів контролю за їх ефективністю;
- забезпечити захист державної таємниці;
- розширювати міжнародне співробітництво України в галузі розвитку і безпечного використання інформаційних ресурсів, протидії загрози розв'язання протиборства в інформаційній сфері [6].

Відповідно до чотирьох складових національних інтересів в інформаційній сфері можна виділити і чотири загрози інформаційній безпеці України.

Загрозами конституційним правам і свободам людини й громадянина в галузі духовного життя й інформаційної діяльності можуть бути:

- прийняття органами державної влади нормативних правових актів, які обмежують конституційні права та свободи громадян у галузі духовного життя й інформаційної діяльності;
- створення монополій на формування, одержання й поширення інформації в Україні, зокрема з використанням телекомунікаційних систем;
- протидія, зокрема з боку кримінальних структур, реалізації громадянами своїх конституційних прав на особисту та сімейну таємницю, таємницю листування, телефонних переговорів, інших повідомлень;
- протиправне застосування спеціальних засобів впливу на індивідуальну і суспільну свідомість;

– невиконання органами державної влади та органами місцевого самоврядування, організаціями та громадянами вимог державного законодавства, що регулює відносини в інформаційній сфері;

– неправомірне обмеження доступу громадян до відкритих інформаційних ресурсів органів державної влади та органів місцевого самоврядування, до відкритих архівних матеріалів та іншої відкритої соціально значимої інформації;

– дезорганізація та руйнування системи нагромадження і зберігання культурних цінностей, враховуючи архіви;

– порушення конституційних прав і свобод людини і громадянина в галузі масової інформації;

– витіснення національних інформаційних агентств, засобів масової інформації з внутрішнього інформаційного ринку і посилення залежності духовної, економічної і політичної сфер громадського життя України від закордонних інформаційних структур;

– девальвація духовних цінностей, пропаганда зразків масової культури, культу насильства;

– зниження духовного, морального і творчого потенціалу населення України, що істотно ускладнить підготовку трудових ресурсів для упровадження і використання новітніх технологій, зокрема інформаційних;

– маніпулювання інформацією (дезінформація, приховування чи перекручування інформації).

Загрозами інформаційному забезпеченню державної політики України можуть бути:

– монополізація інформаційного ринку України, його окремих секторів вітчизняними і закордонними інформаційними структурами;

– блокування діяльності державних засобів масової інформації з інформування громадськості в Україні та за її межами;

– низька ефективність інформаційного забезпечення державної політики унаслідок дефіциту кваліфікованих кадрів, відсутності системи формування і реалізації державної інформаційної політики.

Загрозами розвитку вітчизняної індустрії інформації, включаючи індустрію засобів інформатизації, телекомунікації і зв'язку, забезпеченню потреб внутрішнього ринку в її продукції і виходу цієї продукції на світовий ринок, а також забезпеченню накопичення, зберігання та ефективного використання вітчизняних інформаційних ресурсів можуть бути:

– протидія доступу України до новітніх інформаційних технологій, рівноправній участі виробників у світовому розподілі праці в індустрії інформаційних послуг, засобів інформатизації, телекомунікації і зв'язку, інформаційних продуктів, а також створення умов для посилення технологічної залежності України в галузі сучасних інформаційних технологій;

– закупівля органами державної влади імпортованих засобів інформатизації, телекомунікації і зв'язку при наявності вітчизняних аналогів, що за своїми характеристиками не поступаються закордонним зразкам;

– витіснення з вітчизняного ринку виробників засобів інформатизації, телекомунікації і зв'язку;

– збільшення відтоку з України фахівців і суб'єктів інтелектуальної власності [7].

Загрозами безпеці інформаційних і телекомунікаційних засобів і систем є:

- протиправне збирання та використання інформації;
- порушення технології обробки інформації;
- упровадження в апаратні та програмні вироби компонентів, які реалізують функції, не передбачені документацією на ці вироби;
- розробка й поширення програм, що порушують нормальне функціонування інформаційно-телекомунікаційних систем, зокрема систем захисту інформації;
- радіоелектронний вплив із метою виведення з ладу, пошкодження чи руйнування засобів і систем обробки інформації, телекомунікації та зв'язку;
- вплив на парольно-ключові системи захисту автоматизованих систем обробки та передачі інформації;
- компрометація ключів і засобів криптографічного захисту інформації;
- витік інформації технічними каналами;
- упровадження електронних пристроїв для перехоплення інформації у технічні засоби обробки, зберігання та передачі інформації з каналів зв'язку і у службові приміщення органів державної влади, організацій усіх форм власності;
- знищення, пошкодження, руйнування чи розкрадання машинних та інших носіїв інформації;
- перехоплення інформації в мережах передачі даних та лініях зв'язку, дешифрування цієї інформації та нав'язування хибної інформації;
- використання несертифікованих вітчизняних і закордонних інформаційних технологій або засобів захисту інформації при створенні й розвитку інформаційної інфраструктури;
- несанкціонований доступ до інформації в банках і базах даних;
- порушення законних обмежень на поширення інформації.

Головний консультант, відділу інформаційної безпеки та міжнародних інформаційних відносин Національного інституту проблем міжнародної безпеки Ради національної безпеки і оборони України Д. Дубов вважає, що ступінь інформаційної безпеки значною мірою визначається рівнем розвитку національної інформаційної інфраструктури захисту інформації [8] (рис. 3).



Рис. 3. Структура компонентів національної інфраструктури захисту інформації

Загальні методи забезпечення інформаційної безпеки України можна поділити на правові, організаційно-технічні й економічні.

До правових методів забезпечення інформаційної безпеки України належать розробка нормативних правових актів, що регламентують відносини у інформаційній сфері, і нормативних методичних документів із питань забезпечення інформаційної безпеки України. Найважливішими напрямками цієї діяльності є:

- внесення змін і доповнень до законодавства України, що регулює відносини в галузі забезпечення інформаційної безпеки, з метою створення й удосконалення системи забезпечення інформаційної безпеки України, усунення внутрішніх протиріч у державному законодавстві, протиріч, пов'язаних із міжнародними угодами, до яких приєдналася Україна, а також з метою конкретизації правових норм, що встановлюють відповідальність за правопорушення в галузі забезпечення інформаційної безпеки України;

- законодавче розмежування повноважень у галузі забезпечення інформаційної безпеки України між органами державної влади, визначення цілей, завдань і механізмів участі в цій діяльності громадських об'єднань, організацій і громадян;

- розробка та прийняття нормативних правових актів України, які встановлюють відповідальність юридичних і фізичних осіб за несанкціонований доступ до інформації, її протиправне копіювання, перекручування і протизаконне використання, навмисне поширення недостовірної інформації, протиправне розголошення інформації з обмеженим доступом, використання в злочинних і корисливих цілях службової інформації чи інформації, що містить комерційну таємницю; уточнення статусу іноземних інформаційних агентств, засобів масової інформації та журналістів, а також інвесторів при залученні іноземних інвестицій для розвитку інформаційної інфраструктури України;

- законодавче закріплення пріоритету розвитку національних мереж зв'язку і вітчизняного виробництва космічних супутників зв'язку;

- визначення статусу організацій, що надають послуги глобальних інформаційно-телекомунікаційних мереж на території України, і правове регулювання діяльності цих організацій;

- створення правової бази для формування в Україні системи забезпечення інформаційної безпеки, зокрема її центральних органів та регіональних структур [9].

Організаційно-технічними методами забезпечення інформаційної безпеки України є:

- створення й удосконалення системи забезпечення інформаційної безпеки України; посилення діяльності державних органів виконавчої влади із застосування правових норм, включаючи попередження і припинення правопорушень в інформаційній сфері, а також виявлення, викриття та притягнення до відповідальності осіб, що скоїли злочини та інші правопорушення в цій сфері;

- розробка, використання й удосконалення засобів захисту інформації і методів контролю ефективності цих засобів, розвиток захищених телекомунікаційних систем, підвищення надійності спеціального програмного забезпечення;

- створення систем і засобів запобігання несанкціонованому доступу до інформації, що обробляється, і спеціальним впливам, які призводять до руйнування,



знищення, спотворення інформації, а також зміна штатних режимів функціонування систем і засобів та зв'язку;

- виявлення технічних пристроїв і програм, що загрожують нормальному функціонуванню інформаційно-телекомунікаційних систем, запобігання перехопленню інформації у технічних каналах її витоку, застосування криптографічних засобів захисту інформації під час її обробки та передачі каналами зв'язку, контроль за виконанням спеціальних вимог із захисту інформації;

- сертифікація засобів захисту інформації, ліцензування діяльності в галузі захисту інформації, стандартизація способів і засобів її захисту;

- удосконалення системи сертифікації телекомунікаційного обладнання і програмного забезпечення автоматизованих систем обробки інформації на відповідність вимогам із захисту інформації;

- контроль за діями персоналу в захищених інформаційних системах, підготовка кадрів у галузі забезпечення інформаційної безпеки України;

- формування системи моніторингу показників і характеристик інформаційної безпеки України у найважливіших сферах життя і діяльності суспільства та держави.

Економічні методи забезпечення інформаційної безпеки України містять:

- розробку програм забезпечення інформаційної безпеки України і визначення порядку їх фінансування;

- удосконалення системи фінансування робіт із реалізації правових і організаційно-технічних методів захисту інформації, створення системи страхування інформаційних ризиків фізичних і юридичних осіб.

Отже, завданням державного управління в сфері інформаційної безпеки є створення відповідних правових, організаційних, науково-технічних, економічних, фінансових, методичних та гуманітарних засад регулювання процесу. Враховуючи зміст Хартії про особливе партнерство між Україною та НАТО (1997 р.), можемо виокремити основні напрями державної політики в інформаційній сфері, які необхідно привести у відповідність до стандартів НАТО. Це розвиток демократичних інститутів, зміцнення політичного плюралізму, а також встановлення демократичного контролю над Воєнною організацією держави.

Зважаючи на це, можна окреслити такі завдання для України у галузі забезпечення інформаційної безпеки:

- забезпечення свободи слова, думки та права на інформацію;

- визначення меж свободи поширення інформації (заборона поширення інформації про приватне життя, наклеп, образа, віднесення інформації до категорії з обмеженим доступом);

- правове закріплення статусу засобів масової інформації як незалежних, демократичних інститутів;

- захист інформації з обмеженим доступом;

- закріплення юридичної відповідальності за порушення інформаційного законодавства.

### Література

1. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України “Про інформацію” та статті 12 Закону України “Про прокуратуру” (справа К. Г. Устименка) від 30.10.1997 р. // Офіційний Вісник України [Текст]. — 1997. — № 46. — 24 листоп.

2. Додонов О. Г. Державна інформаційна політика і становлення

інформаційного суспільства в Україні / О. Г. Додонов, О. С. Горбачик, М. Г. Кузнецова // Стратегічна панорама [Текст]. — 2002. — № 1. — С. 6—14.

3. Клименко П. М. Інформація як об'єкт інтелектуальної власності, що потребує охорони / П. М. Клименко // Недержавна система безпеки підприємництва як суб'єкт національної безпеки України [Текст] : зб. матер. наук.-практ. конф. (16 – 17 травня 2001 р., м. Київ). — К. : Європ. ун-т, 2003. — С. 283—289.

4. Андрощук Г. А. Экономическая безопасность предприятия: защита коммерческой тайны [Текст] : монография / Г. А. Андрощук, П. П. Крайнев. — К. : Издательский Дом “Ин Юре”, 2000. — 400 с.

5. Флюр О. М. Інтеграція України у світовий інформаційний простір [Текст] : автореф. дис. на здоб. наук. ступ. канд. політ, наук. 23.00.04 / О. М. Флюр ; Київ. нац. ун-т ім. Т. Шевченка. — К. : [б. в.], 2004. — 18 с.

6. Додонов О. Г. Державна інформаційна політика і становлення інформаційного суспільства в Україні... — С. 11.

7. Морозов О. Інформаційна безпека в умовах сучасного стану і перспективи розвитку державності / О. Морозов // Віче [Текст]. — 2007. — № 12. — Спецвипуск. — С. 23—25.

8. Дубров Д. В. Інформаційна безпека в умовах впровадження електронного врядування [Електронний ресурс] / Д. В. Дубров. — Режим доступу : [http://www.niisp.gov.ua/publication/info/Dubov\\_bezpeka\\_EU\\_BookPalate.pdf](http://www.niisp.gov.ua/publication/info/Dubov_bezpeka_EU_BookPalate.pdf).

9. Бачило И. Л. Информационное право [Текст] : учебник / И. Л. Бачило, В. Н. Лопатин, М. А. Федотов ; под ред. Б. Н. Топорнина. — СПб. : Юридический центр Пресе, 2001. — 789 с.

**L. Yevdochenko**

## **WAYS AND METHODS OF STATE INFORMATIONAL SECURITY PROVISION OF UKRAINE: THEORETICAL ASPECT**

**The theoretical and methodological foundations of information security of Ukraine and its impact on the functioning of public administration of Ukraine, the essence and basic approaches to the definition of national security, the means of its implementation, the ways of ensuring the national security in the sphere of information in Ukraine, the sources of threats to information security of Ukraine, the methods of information security provision of Ukraine at the present stage of social development are considered.**

**Key words: national security, information security, national interests.**