

СТАН ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

У статті проаналізовано стан забезпечення інформаційної безпеки в Україні на основі аналізу Доктрини інформаційної безпеки України, яка затверджена Указом Президента України від 8 липня 2009 року.

Ключові слова: інформаційна безпека, інформаційний простір, інформаційні ресурси, інформаційна інфраструктура, національна безпека.

Постановка проблеми та її актуальність.

В умовах розбудови правової держави, ускладнених глобалізаційних та інтеграційних процесів, проблемою для України є необхідність прискорення формування комплексної системи адміністративно-правового регулювання сфери забезпечення інформаційної безпеки.

Аналіз досліджень та публікацій. Питання інформаційної безпеки стало предметом наукових дискусій у рамках робіт таких вчених, як І. Арістова, І. Березовська, В. Голубєв, В. Гурковський, О. Дзьобань, Р. Калюжний, В. Конах, Б. Кормич, В. Ліпкан, Ю. Максименко, А. Марушак, В. Цимбалюк, О. Юдін, Р. Юсупов та ін.

Проте зазначені дослідження та наукові праці містять лише фрагментарні наукові розробки у сфері забезпечення інформаційної безпеки України. Проблема обґрунтування стану забезпечення інформаційної безпеки України залишається практично не дослідженою.

Метою нашого дослідження є визначення стану забезпечення інформаційної безпеки на основі аналізу Доктрини інформаційної безпеки України, формування на цій основі пропозицій теоретичного значення, а також науково-обґрунтованих рекомендацій, спрямованих на підвищення його ефективності.

Виклад основного матеріалу. Інформаційна безпека є складним соціальним і політико-правовим феноменом, важливою складовою всіх сфер забезпечення національної безпеки. Стан інформаційної безпеки доцільно розглядати як захищеність національних інтересів та спроможність нейтралізувати чи послабити дію внутрішніх і зовнішніх потенційних і реальних інформаційних загроз, які можуть бути застосовані проти України. Система забезпе-

чення інформаційної безпеки має включати комплекс превентивних заходів із надання гарантій захисту життєво важливих інтересів особи, суспільства, держави, своєчасне і адекватне реагування на увесь спектр інформаційних безпеченних чинників з метою захисту національних інтересів та національної безпеки.

Указом Президента України від 8 липня 2009 року затверджена Доктрина інформаційної безпеки України [1]. Прийняття цього державного акту – актуальна потреба часу, так як сфера інформаційної безпеки країни й досі залишається найбільш нерегульованою в правовому, організаційному, методичному, науково-технічному, кібербезпековому та інших напрямках діяльності. Наведена Доктрина затверджена через шість років після прийняття Закону України «Про основи національної безпеки України» [2], який передбачає комплексне вирішення завдань та формування системи захисту національних інтересів. Законом встановлено, що на підставі його правових норм (ст. 2) розробляються і затверджуються Президентом України стратегії, доктрини, концепції, програми тощо.

Доктрина інформаційної безпеки України 2009 року містить наступні розділи: Загальні положення. 1. Основні засади інформаційної безпеки. 2. Інформаційна безпека в системі забезпечення національної безпеки. Цей розділ містить наступні підрозділи: життєво важливі інтереси в інформаційній сфері; реальні та потенційні загрози інформаційній безпеці України. 3. Напрями державної політики у сфері інформаційної безпеки України. 4. Прикінцеві положення.

Першим розділом Доктрини є «Загальні положення». Зміст цього розділу має поверхову нейтральну характеристику сучасного світу без будь-якого зв'язку зі станом інформаційної безпеки України. Характерною ознакою Докт-

рини є відсутність в жодному з її розділів оцінки стану інформаційної безпеки нашої країни. А це не дає можливості визначитися щодо позитивних здобутків та невирішених проблем у цій важливій сфері забезпечення національної безпеки, тобто з якого реального стану інформаційної безпеки доцільно починати відлік удосконалення правового, організаційного, науково-методичного, матеріально-технічного тощо забезпечення державної політики у цій сфері діяльності.

Процитуємо перший абзац першого розділу: «За умов глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень і боротьби різновекторних національних інтересів держав стає інформаційний простір. Сучасні інформаційні технології дають змогу державам реалізувати власні інтереси без застосування військової сили, послабити або завдати значної шкоди безпеці конкурентної держави, яка не має дієвої системи захисту від негативних інформаційних впливів. Зупинимось на найбільш важливих помилках розробників Доктрини, викладених у цьому розділі, які дезінформують державні інституції та суспільство.

До головної визначальної причини сучасного інформаційного протиборства віднесена «глобальна інтеграція та жорстка конкурентна боротьба». Це лише одна із складових необхідності забезпечення інформаційної безпеки і не сама головна. Глобальні інтеграційні процеси та конкурентна боротьба, в тому числі міжнародна, були характерними і для індустріального етапу розвитку. Якісно нові ризики, виклики, загрози і небезпеки щодо інформаційної безпеки породжені інформаційною епохою розвитку цивілізації. Інформація, інформаційні технології перетворилися на потужні засоби досягнення визначених цілей щодо розвитку політичних і соціально-економічних систем, забезпечення панування наддержав, союзів або об'єднань держав над недостатньо розвинутими країнами та цілими регіонами.

Розробники Доктрини виявили недостатній рівень знань у сфері психології, політології, інформаційних технологій тощо при визначенні змісту інформаційної боротьби, що є реаліями сучасного світу. В цьому розділі йдеться про те, що сучасні технології дають змогу державам реалізувати власні інтереси без застосування військової сили, послабити або завдати значної шкоди безпеці конкурентної

держави, яка не має дієвої системи захисту від негативних інформаційних впливів. Наведене положення визначає лише зовнішній аспект інформаційної боротьби, уникає від орієнтування суспільства і держави на усунення або послаблення дії внутрішніх інформаційних війн на сталий розвиток країни, стабільність та добробут населення. Повною недоречністю є положення про те, що інформаційні технології дають змогу державам реалізувати власні інтереси без застосування військової сили. Тобто, країні достатньо володіти сучасними інформаційними технологіями і немає необхідності постійно здійснювати вдосконалення Збройних Сил держави. Це не розуміння або ігнорування подій сучасного світу, пов'язаних із застосуванням військової сили провідними країнами світу, та внутрішньодержавними військовими конфліктами в різних регіонах планети. Застосуванням військової сили завжди передують широкомасштабні інформаційні війни як найвища ступінь інформаційного протиборства.

Автори Доктрини не відійшли від міфотворчості у сфері державної політики щодо інформаційної безпеки. Обсяг, швидкість та якісь обробки інформації, тобто потрібно вважати – інформатизацію розглядають як засіб лікування всіх політичних, економічних, соціальних, управлінських, оборонних та інших проблем без будь-яких зв'язків з інформаційною безпекою. Державна політика забезпечення національної безпеки в цій важливій сфері має передбачати комплекс превентивних, скоординованих за місцем і часом заходів для захисту від негативних інформаційних впливів на особу, суспільство і державу, всіх її структур, а також інформаційно-телекомунікаційні системи з їх обсягами, швидкістю та якістю обробки інформації. Безпідставно автори Доктрини визначають функціональне навантаження інформаційних технологій та нерозуміння їх ролі в сфері оборони і воєнного будівництва. Не інформаційними технологіями, а Воєнною доктриною України, положення якої реалізуються відповідними актами законодавства, визначається «структура» воєнної організації держави, її збройних сил, «якість озброєнь і рівень їх достатності».

У «Загальних положеннях» Доктрини та інших її розділах не тільки не враховуються, а фактично упущені визначальні положення сучасної геополітики, яка відмовляється від домінування суто географічних факторів і у

зв'язку з цим змінює змістовну сутність поняття «національна безпека» та її складових.

Геополітичні пріоритети і сценарії розвитку України всебічно обґрунтовані в монографії вченими НІСД і Національного інституту українсько-російських відносин [3]. Зупинимось на головних положеннях щодо інформаційної безпеки, визначених авторами монографії.

Нова геополітика розглядає національну безпеку в цілому, тобто і її складову – інформаційну безпеку, не тільки як стан захищеності людини, суспільства, держави від певних загроз, а як систему оптимізації взаємовідносин між усвідомленими загрозами та ресурсами, що має суспільство для протидії цим загрозам.

Фактором, що послаблює здатність держави нейтралізувати загрози, є посилення взаємозалежності країн та їх відкритість до зовнішніх впливів. Здебільшого держава перестає бути монополістом на власній території, її інформаційна політика все більш обмежується, корегується, нівелюється діями інших держав, міжнародних організацій, недержавних організацій, неформальних об'єднань негативної спрямованості, кримінальних угруповань тощо. Слабка ідеологічно, інституційно, економічно держава не здатна скористатися технологічними, економічними, соціокультурними перевагами глобалізації, проте активно приймає її негативні риси. На думку авторів монографії [3] – це шлях назад у становленні і стабільності державної влади, невинного посилення позадержавних джерел політичного та економічного впливу, переходу технологічної відсталості у стратегічну ерозію національної ідентичності.

Таким чином, аналіз змісту «Загальних положень» Доктрини свідчить про те, що вони відірвані від реалій сучасної інформаційної епохи, загроз національним інтересам у зв'язку із широким розвитком інформаційних технологій, інформаційно-телекомунікаційних систем та процесів глобалізації. Безумовно і недбало викладені положення цього розділу, їх відірваність від реалій сучасності дезінформує суспільство, державні інституції щодо державної політики у сфері інформаційної безпеки України.

Зміст другого розділу визначає лише окремі керівні основи забезпечення інформаційної безпеки України. До основної мети реалізації положень Доктрини віднесено створення в Україні розвинутого національного інформаційного простору і захист її інформаційного суверенітету. Із наведеного положення випли-

ває декілька висновків: 1) до засад інформаційної безпеки має відношення лише захист інформаційного суверенітету; 2) формування національного інформаційного простору – це сфера державної інформаційної політики, а інформаційна безпека має полягати в забезпеченні безпечного функціонування інформаційного простору в процесі його розвитку, тобто захисті всіх структурних елементів, що до нього входять та суб'єктів, які в ньому діють; 3) поза сферою основних засад інформаційної безпеки залишилися інформаційні складові забезпечення національної безпеки, захисту національних інтересів тощо.

Дезінформуванням державних інституцій та суспільства є визначення принципом забезпечення інформаційної безпеки «економічну доцільність». Виникають питання: у яких економічних критеріях можна вимірювати захист прав, свобод та безпеки людини, захист духовних та моральних цінностей, своєчасність і адекватність заходів захисту реальним і потенційним загрозам тощо?

Уважне вивчення змісту Зводу відомостей, що становлять державну таємницю України [4], свідчить про те, що понад третини статей Зводу передбачають захист інформації з боку держави в інтересах національної безпеки з витратою безповоротних коштів.

Відомий український учений О. Гончаренко, розглядаючи особливості і пріоритети політики і стратегії національної безпеки, вважає економічну доцільність в цій сфері невинною в своїй основі. Він пише: «Національна безпека завжди була і буде найбільш збитковою категорією витрат нації (держави). За національну безпеку, незалежність і волю треба платити і платити дорого. Якщо потрібно – кров'ю кращих синів і дочок нації. Безкоштовної національної безпеки не буває. Безкоштовним може бути лише ярмо раба на шії» [5, с. 118 – 127].

Таким чином, положення другого розділу Доктрини орієнтують на вирішення важливих проблем у сфері забезпечення інформаційної безпеки, однак лише за окремими напрямками. Зміст основних засад державної політики щодо цієї сфери діяльності викладено не на належному рівні і не дозволяє забезпечити розуміння і вдосконалення системи інформаційної безпеки особи, суспільства, держави.

Аналіз життєво важливих інтересів особи, суспільства, держави у третьому розділі Докт-

рини є підставою для висновків про те, що вони визначені без зв'язку з реаліями сучасного світу, тенденціями зростання загроз інформаційної безпеки, її реальним станом в Україні, не враховують позитивні і негативні аспекти державної політики щодо забезпечення їх реалізацій і захисту. Окрім того, інформаційна безпека в системі забезпечення національної безпеки передбачає захист життєво важливих інтересів лише у власне інформаційній сфері, що звужує розуміння як теоретичних, так і практичних аспектів інформаційної безпеки.

І саме головне. Визначення національних інтересів, яким загрожує інформаційна небезпека, є основою для розробки і вдосконалення державної політики у сфері інформаційної безпеки. В умовах невизначеності національної ідеї, а суспільство розколото за політичними, економічними, соціальними, територіальними, етнічними, релігійними, екологічними параметрами, система національних інтересів має включати зрозумілі для широких верств населення, несуперечні, взаємоузгоджені життєво важливі матеріальні, інтелектуальні, духовні цінності. Національні інтереси в умовах сучасної України не можуть бути джерелом політичного, ідеологічного протистояння, економічної нестабільності та інших негативних процесів і явищ. Національні інтереси мають об'єднувати український народ.

Національні інтереси повинні розроблятися на підставі вимог Конституції України, чинного законодавства та загальноновизнаних ціннісних орієнтирів. При цьому доцільно враховувати те, що відповідно до Основного Закону України (ст. 17) суспільне життя в Україні ґрунтується на засадах політичної, економічної та ідеологічної багатоманітності, що жодна ідеологія не може вважатися державою як обов'язкова, що державою гарантується свобода політичної діяльності, не заборонена Конституцією і законами України. Наведені положення Основного Закону України є загальноновизнаними у цивілізованому світі підходами для будівництва і розвитку демократичної, правової держави. В Україні заборонено визнавати жодну ідеологію як державну, а гарантування політичної діяльності використовується громадськими організаціями, прихильниками різних політичних та ідеологічних поглядів, для боротьби без огляду на неминучі негативні наслідки.

Основою для розроблення національних інтересів і закріплення їх у масовій свідомості є

Конституція України і сучасне конституційне право. Відомі українські вчені Ю. М. Тодика і В. С. Журавський підкреслюють: «В умовах становлення України як демократичної, соціальної, правової держави дедалі зростає його роль в оптимізації та прискоренні процесів державотворення і правотворення. Щоб ці процеси були керованими, прогнозованими і відповідно ефективними й оптимальними, вони мають ґрунтуватися на наукових засадах, здобутках та рекомендаціях науки конституційного права» [6]. Теорією науки конституційного права обґрунтовано: «Засади конституційного ладу країни відображають прагнення людини і суспільства до щастя, добра, справедливості, свободи, рівності, солідарності, гуманізму, демократії та порядку. У засадах конституційного ладу, як правило, закріплюється суспільний ідеал» [Там само, с. 83].

Відповідно до висновків, викладених у монографії [3], учених НІСД та національного інституту російсько-українських відносин: «...самоузгоджений комплекс національних інтересів, пріоритетів і цілей міг би відігравати їх роль і сприяти консолідації суспільства навколо загальнолюдських цінностей, таких як «виживання», «добробут», «рівноправність», «свобода», «розвиток», «справедливість», які є зрозумілими і прийнятними для будь-якої людини». І далі: «Національні інтереси та співвіднесені з ними цінності й цільові настанови мають складати основу будь-якої інтегральної стратегії національної безпеки на перспективу, ефективну імплементацію якої повинні забезпечувати спільні зусилля виконавчої та законодавчої гілок влади».

Пріоритети національних інтересів України закріплені Законом України «Про основи національної безпеки України», прийнятим Верховною Радою України у 2003 році. Через шість років Доктриною інформаційної безпеки України життєво важливі інтереси особи, суспільства, держави не впливають із пріоритетних національних інтересів, визначених Законом, стосуються лише власне інформаційної сфери та викладені абстрактно і соціально-беззмістовно. Доктрина, введена в дію через такий проміжок часу після прийняття Закону, повинна була враховувати як позитивні надбання, так і проблемні аспекти щодо розвитку змістовної сутності національних інтересів, забезпечення яких має здійснюватися державною політикою інформаційної безпеки. Не-

припустимо, коли в державі Верховна Рада, Президент і Уряд бачать різний зміст національних інтересів України.

Однією із небезпечних загроз національним інтересам будь-якої сфери суспільного життя і державотворення є невизначеність у правовому і організаційному плані системи інформаційного забезпечення політики держави. Це важлива складова забезпечення інформаційної безпеки як складової національної безпеки. Фактично в Україні ці проблеми вирішуються окремими державними організаціями на свій розсуд. В нашій країні відсутня ієрархічно побудована організаційна структура державних органів від вищих ланок гілок влади до громадянина з чітким визначенням соціально уповноважених органів, які організують і координують цю діяльність у сфері інформаційної безпеки. Це одна з причин поразки і втрат державної політики України як на міжнародній арені, так і у внутрішніх справах, а також невиконання настанов чинного законодавства.

Так, Конституція України до найважливішої функції держави, справи всього українського народу відносить «захист суверенітету і територіальної цілісності України» (ст. 17). Закон України «Про основи національної безпеки України» визначає як загрозу національним інтересам та національній безпеці посягання на територіальну цілісність, територіальні претензії з боку інших держав (ст. 7). У зв'язку з цим виникає питання такого змісту: чому Україна програла судовий процес Румунії щодо морського шельфу в районі о. Зміїний Чорного моря? Відповідь очевидна – процес було програно на етапі ще підготовки до нього. Однією з причин була відсутність інформаційного забезпечення захисту територіальної цілісності України. В Румунії навпаки – була розгорнута агресивна інформаційна кампанія проти України, в якій брали участь вищі посадові особи держави, державні органи, громадські організації. У суспільстві і у міжнародній спільноті сформувалися відповідні погляди щодо неправомірності територіального розмежування з Україною. Ця кампанія триває й досі щодо територіального розмежування.

Окремому розгляду підлягає така загроза інформаційній сфері, як витік і 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. Про цю загрозу відмічається в багатьох державних рішеннях, правових актах, а також у Законі України «Про основи національної безпеки України». І така загроза існує. Одна із головних причин в тому, що в процесі адміністративних реформ в нашій країні була втрачена функція державного управління, а саме: розробки державної політики щодо інформації обмеженого доступу, що не становить державної таємниці, організації і координації діяльності в цій сфері. Наведена сфера залишається не врегульованою ні в правовому, ні в організаційному плані. Обмеження доступу до такої інформації встановлені підзаконними актами на порушення вимог Основного закону України [7, 8]. А це створює передумови як для порушення прав громадян і суспільних організацій щодо одержання і використання такої інформації, так і для її знеособлення і витоку. В Україні з 1996 року відсутній державний орган з повноваженнями організації і координації діяльності у цій сфері. В положеннях про центральні та регіональні державні адміністрації також залишаються не визначеними їх функції щодо захисту інформації обмеженого доступу, що не становить державної таємниці.

Реальні та потенційні загрози інформаційній безпеці здебільшого визначені абстрактно у відриві від їх джерел. А це не дає можливості виконавцям Доктрини забезпечити адресність адекватних заходів, спрямованих на ліквідацію загроз або послаблення їх дії. Наприклад: поширення у світовому інформаційному просторі викривленої, недостовірної інформації про Україну; несанкціонований доступ до інформаційних ресурсів органів державної влади; негативні інформаційні впливи, в тому числі із застосуванням спеціальних засобів, на індивідуальну та суспільну свідомість. Наведені загрози та багато інших закономірно ставлять запитання про джерела загроз, тому що це є підставою для визначення державних інституцій, які мають впроваджувати відповідні захисні заходи. Принциповим є питання і про класифікацію загроз за зовнішніми і внутрішніми ознаками. Без цього є проблематичним визначити сили, засоби і заходи протидії загрозам, а саме: інформаційні, правові, організаційні, економічні, інженерно-технічні, дипломатичні, спеціальної спрямованості та інші.

Є два варіанти вирішення підходу до визначення загроз та їх джерел. Перший – в одному

розділі кожен загрозу визначати у зв'язку з її джерелом. Другий – інформаційні загрози та їх джерела визначити окремими розділами. Наприклад, в Доктрині інформаційної безпеки Російської Федерації види загроз та їх джерела визначені окремими розділами. Російська Доктрина має спеціальний розділ, який характеризує стан інформаційної безпеки і основні завдання щодо її забезпечення [9]. Вважаємо, що без оцінки позитивних здобутків та невирішених проблем у цій сфері проблематично визначити напрями вдосконалення системи інформаційної безпеки та узгодженість і взаємодію державних інституцій щодо підтримання її на необхідному рівні.

Четвертий розділ Доктрини з метою забезпечення інформаційної безпеки передбачає, що держава має «вживати» заходів у сферах: зовнішньополітичній, державної безпеки, воєнній, внутрішньополітичній, економічній, соціальній та гуманітарній, науково-технологічній, екологічній. Окремою сферою власне інформаційну з питань впровадження заходів державної політики інформаційної безпеки цей розділ необґрунтовано не передбачає. Заходи стосовно цієї сфери розпорочені за іншими сферами життєдіяльності особи, суспільства і держави, і лише частково забезпечуватиме захист національних інтересів в інформаційній сфері. Понад 70 відсотків заходів державної політики інформаційної безпеки стосуються власне інформаційної сфери; більшість з них мають реалізовуватися в межах державної інформаційної політики, а саме: формування національних інформаційних ресурсів, діяльність ЗМІ, інформатизація, входження у світовий інформаційний простір та інші. Отже, державна політика, визначена Доктриною, лише частково спрямована на забезпечення інформаційної безпеки України та її національних інтересів. У деяких сферах життєдіяльності особи, суспільства і держави заходи державної політики вузькі за своїм змістом. Визначальні системоутворюючі напрями державної політики з питань інформаційної безпеки залишилися поза увагою Доктрини.

У зовнішньополітичній сфері з п'яти заходів чотири – це напрями, що мають реалізовуватися державною інформаційною політикою.

На сучасному етапі розвитку гострого значення набуває міжнародна інформаційна безпека. Ще у серпні 2000 року Всесвітня організація учених на своїй 25-й сесії у переліку загроз людству на перше місце поставила загрозу міжнародній інформаційній безпеці. Декілька разів Гене-

ральна Асамблея ООН закликала світову спільноту обговорити проблему і прийняти рішення по усуненню можливості використання інформації в цілях не сумісних із забезпеченням безпеки людства. Прийняття таких рішень блокувалося державами, що домінують в інформаційній сфері і здійснюють активну розробку інформаційної зброї [10]. Тому участь України в двосторонніх і багатосторонніх міжнародних структурах забезпечення як регіональної, так і власної інформаційної безпеки, є актуальним напрямом державної політики у цій галузі.

Важливою теоретичною і практичною складовою Доктрини інформаційної безпеки України має бути визначення функцій суб'єктів щодо забезпечення інформаційної безпеки. Реальністю є те, що в Україні залишається досі не сформована логічно завершена система державного управління в цій важливій сфері національної безпеки. Виконуються лише окремі функції деякими державними органами, незважаючи на політико-правові рішення з цих питань, певні наукові дослідження і публікації у відповідних виданнях. Загальнодержавна координація діяльності суб'єктів, що забезпечують реалізацію державної політики інформаційної безпеки, потребує удосконалення.

Висновки. Зміст Доктрини інформаційної безпеки України 2009 року не дає повного уявлення про сукупність офіційних поглядів, цільових настанов, керівних принципів, напрямів діяльності, спрямованих на реалізацію державної політики інформаційної безпеки з метою своєчасного виявлення, відвернення і нейтралізації реальних і потенційних загроз. Доктрина не визначає важливі аспекти забезпечення інформаційної безпеки України, а саме: функції щодо реалізації державної політики у цій важливій складовій забезпечення національної безпеки; організаційну структуру державних органів, інших суб'єктів та їх повноваження щодо реалізації державної політики у цій сфері; порядок координації діяльності суб'єктів з питань забезпечення інформаційної безпеки особи, суспільства і держави. Документ не визначає загроз життєво важливим інтересам і напрямам діяльності, спрямованих на підготовку сил і засобів для активних дій в процесі можливих інформаційних протистоянь із супротивниками і конкурентами, попередження інформаційної агресії та застосування проти України інформаційної зброї та інших негативних інформаційних впливів. Забезпечення інформаційної безпеки України Док-

триною передбачено лише через засади, заходи і засоби власне інформаційної сфери, тобто сфери обігу інформації і діяльності ЗМІ. Засади державної політики в цій важливій сфері слугуватимуть основою для розробки і впровадження стратегій, доктрин, програм, планів забезпечення інформаційної безпеки на відповідних напрямках життєдіяльності особи, суспільства, держави.

Перспектива подальших досліджень. Особливу увагу дослідників і практиків слід звернути на необхідність розробки проблематики напрямів державної політики забезпечення інформаційної безпеки у сферах: економіки, зовнішньополітичній, внутрішньополітичній, у сфері оборони, державної безпеки, соціально-гуманітарній, науково-технологічній, екологічній, інформаційній тощо.

Література

1. *Доктрина* інформаційної безпеки України: Затверджено Указом Президента України від 08.07.2009 № 514/2009 // Офіційне інтернет-представн. Президента України. – 30.01.2010.file://g. – С. 1-8.

2. *Про основи* національної безпеки: Закон України № 964-IV від 10.06.2003 // Урядовий кур'єр. – 2003. – 30 лип.

3. *Україна 2000 і далі: геополітичні інтереси та сценарії розвитку: Монографія* / Автор. колектив: О. М. Гончаренко (керівник), Б. О. Парахонський, Р. Н. Жангожа та ін. – К.: НІСД, 1999. – С. 9-46.

4. *Звід* відомостей, що становлять державну таємницю України: Затверджено наказом СБ України від 12.08.2005 № 52 // Офіційний вісник України. – 2005. – 9 лют.

5. *Гончаренко О.* Стратегія національної безпеки України: геополітичні пріоритети та регіональні реалії / О. Гончаренко // Зб. ст. за матер. Міжнародної конф. «Стратегія національної безпеки України в контексті досвіду світової спільноти», Київ, 9 – 10.2000 р. – К.: Сатсанга, 2001. – С. 118-127.

6. *Конституційне* право України: Підручн. для студентів вищих навч. закладів / За заг. ред. Ю. М. Тодики, В. С. Журавського. – К.: Вид. Дім «ІнЮре», 2002. – 544 с.

7. *Інструкція* про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави: Затверджено Постановою Кабінету Міністрів України від 27.11.1998 № 1893 із змінами та доповненнями // Інформаційні технології. Нормативна база. – К.: КНТ, 2005. – 500 с.

8. *Інструкція* про порядок охорони державної таємниці, а також іншої інформації з обмеженим доступом, що є власністю держави, під час прийому іноземних делегацій, груп та окремих іноземців і проведення роботи з ними: Затверджено Постановою Кабінету Міністрів України від 22.05.1996 № 558 // Інформаційні технології. Нормативна база. – К.: КНТ, 2005. – 500 с.

9. *Доктрина* информационной безопасности Российской Федерации: Утверждена Президентом РФ 09.09.2000 // Российская газета. – 2000. – 28 сент.

10. *Федоров А.* Семь тезисов противников «Международной информационной безопасности» / А. Федоров // Международная жизнь. – 2001. – № 12. – С. 89 – 92.

О. В. Олейник

Состояние обеспечения информационной безопасности в Украине

В статье проанализировано состояние обеспечения информационной безопасности в Украине на основе анализа Доктрины информационной безопасности Украины, которая утверждена Президентом Украины от 8 июля 2009 года.

Ключевые слова: информационная безопасность, информационное пространство, информационные ресурсы, информационная инфраструктура, национальная безопасность.

О. Олійник

The State of Information Security in Ukraine

The article analyzes the state of the information security in Ukraine in light of the Information Security Doctrine of Ukraine which was approved by the President's Decree of July 8, 2009.

Key words: information security, principles of the informational security, information infrastructure, national security.