КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН ТА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

До 85-річчя Київського національного університету внутрішніх справ присвячується

В. А. ЛІПКАН, Ю. Є. МАКСИМЕНКО, В. М. ЖЕЛІХОВСЬКИЙ

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ЄВРОІНТЕГРАЦІЇ

НАВЧАЛЬНИЙ ПОСІБНИК *Серія:*

Національна і міжнародна безпека

Київ
КНТ
2006

ББК 67.ї)(І Vioao 1.1.) **УДК** .4
1(1 77)
.11 (і І

Рецензенти:

('. Я. Жук — начальник кафедри інформаційної боротьби І Іаціші альної академії оборони України, доктор технічних наук, професор;

П. Я. Пригунов — директор науково-дослідного інституту проблем безпеки, кандидат психологічних наук, доцент.

В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський

Л **61** **Інформаційна безпека України в умовах євроінтеграції:** Навчальний посібник. — К.: КНТ, 2006. — 280 с. (Серія: Національна і міжнародна безпека)

ISBN 966-373-116-8

Даний глосарій — одна з небагатьох спроб осмислити феномен національної безпеки з позицій системного підходу. У ньому зібрані основні поняття і терміни, які використовуються при викладанні безпекових дисциплін з урахуванням необхідності дослідження національної безпеки в межах окремої навчальної дисципліни « Націобезпекознавство ».

Основна термінологія даного глосарію успішно апробована в Академії управління МВС України, Інституті права і безпеки підприємництва Європейського університету, використана в Міжнародній поліцейській енциклопедії.

Глосарій призначений для фахівців в галузі національної та міжнародної безпеки, а також тих, кого хвилюють проблеми формування системи знань про національну безпеку, як складову міжнародної безпеки, і її забезпечення в умовах глобалізації.

ББК 67.9(4Ук)301.15

ISBN 966-373-116-8

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ЄС — Європейський Союз.
ЗНБ — забезпечення національної безпеки.
ІБ — інформаційна боротьба.
ІТ — інформаційні технології.
НБЗ - національнобезпекознавство.
СНБ - система національної безпеки.

ЗМІСТ

ПЕРЕДМОВА

Становлення інформаційної цивілізації потребує докорінної зміни ставлення не лише до формування інформаційної політики, а в її межах політики інформаційної безпеки, що містить вивчення та опанування теоретичних підвалин даних процесів.

Стрибкоподібний розвиток демократичних процесів, помітне збільшення напруги у геополітичному просторі світу, безпекотрансформаційні процеси, внаслідок яких формується нова геобезпекова конфігурація світу, активізація процесів формування інформаційного суспільства потребують адекватної реакції як наукового, так і педагогічного співтовариства.

Декларація України про намір входження до євроатлантичних структур, прагнення вступу до Всесвітньої торговельної організації, а також намагання створити регіональну систему безпеки, яка б стала основою загальноєвропейської системи безпеки, спричинили небувалу хвилю проведення проти нашої держави інформаційних операцій різного рівня інтенсивності.

Відтак, важливого значення у процесі становлення інформаційного суспільства в Україні набувають питання формування національно орієнтованої інформаційної політики з урахуванням кращих європейських взірців у цій сфері.

Недостатнє вивчення цього питання українськими дослідниками, необхідність більш широкого залучення до розв'язання кола зазначених проблем молоді й спонукало авторів до написання даного навчального посібника «Інформаційна безпека України в умовах євроінтеграції».

Системно (макрорівень) ця навчальна дисципліна входить до циклу націобезпекознавчих дисциплін, поряд з такими, як «Теорія національної безпеки (націобезпекознавство)», «Національна безпека України», «Інформаційна безпека України», «Державна інформаційна політика», «Воєнна безпека України», «Безпекознавство», «Економічна безпека України», «Міжнародна безпека», «Право національної безпеки», «Право

міжнародної безпеки», «Право європейської безпеки», «Сили спеціальних операцій», «Основні системи безпеки сучасності» тощо, які мають викладатися на кафедрі національної та міжнародної безпеки. Місце даного курсу в системі націобезпекоз-навчих дисциплін обумовлено євро- інтеграційними прагненнями України.

Архітектоніка (мезорівень) відповідає націобезпекознавчому підходу, обумовлена специфікою об'єкта дослідження і становить собою 10 взаємопов'язаних розділів, які у своїй органічній сукупності закладають підвалини для формування цілісного уявлення про інформаційну безпеку України та Європи, а також підходи до підвищення ефективності функціонування систе,ми забезпечення інформаційної безпеки України в контексті євроін-теграції.

Структурно (мікрорівень) кожний розділ являє собою лекційний матеріал до теми. Складовими розділу є *вступ,* у якому обґрунтовується необхідність аналізу даної теми, її зв'язок із загальною темою навчальної дисципліни, *основні питання,* в яких розкривається зміст розділу, *висновок,* в якому підбивається підсумок розглядуваного матеріалу.

З урахуванням підвищення вимог до теоретичної освіти, у кінці кожного розділу нами запропоновано перелік *ключових понять і термінів* до теми, при чому для полегшення роботи студента, усі визначення надаються у відповідному тезаурусі в кінці підручника.

Мета дисципліни:

• ознайомити з основними проблемами сучасної інформаційної політики, становлення інформаційного суспільства в Україні та Європі;

• розкрити сутність і значення системи забезпечення інформаційної безпеки, розглянути європейський досвід розв'язання даних питань;

• ознайомити студентів з основними проблемами формування інформаційного суспільства в Європі;

• сформувати уявлення про основні напрями здійснення де ржавної інформаційної політики в Україні та Європі.

Завдання дисципліни:

• надати знання щодо сучасних особливостей здійснення державної інформаційної політики в Україні та інших країнах світу;

• ознайомити слухачів з основними концепціями забезпечення інформаційної безпеки України та Європи;

• надати базові знання з таких важливих питань інформаційної безпеки, як сутність та зміст інформаційної безпеки, національні інтереси в інформаційній сфері, інформаційна безпека Євросоюзу, безпека інформаційного суспільства Євросоюзу, адаптація стандартів Євросоюзу до українського інформаційного законодавства;

• сформувати у слухачів уміння та навички щодо аналізу та формування критеріїв адаптації стандартів Європи у сфері інформаційної політики до України.

Після вивчення дисципліни слухачі повинні:

• розробляти пропозиції щодо визначення стратегічних цілей і завдань щодо розвитку інформаційного суспільства в Україні;

• контролювати виконання заходів по реалізації інформаційної політики, виконання законодавчих та підзаконних актів в обумовлені терміни;

• забезпечувати інформаційну безпеку, виходячи з націо нальних інтересів в інформаційній сфері, потенційних і реаль них загроз та небезпек, а також європейських стандартів здійс нення цієї діяльності;

• готувати рекомендації, пропозиції до проектів зовнішньо та внутрішньополітичних стратегій України, спрямованих на адекватну відповідь реальним та потенційним загрозам національній безпеці України;

• визначати вплив факторів зовнішнього та внутрішнього інформаційного середовища на діяльність органів державної влади, імідж країни;

• вміти використовувати понятійно-категорійний апарат при аналізові інформаційної сфери національної безпеки, виборі та реалізації концептуальних підходів із забезпечення інформаційної безпеки;

• вміти формувати доктрину інформаційної безпеки на підставі аналізу положень інформаційної політики України та європейських стандартів з урахуванням методології адаптації законодавства у зазначеній сфері, а також Концепції національної безпеки;

• вміти формувати алгоритм проведення інформаційних операцій;

• володіти загальними методами виявлення ознак проведення проти України спеціальної інформаційної операції;

• на основі моніторингу та аналізу діяльності органів вла ди пропонувати інформаційні засоби підвищення ефективності діяльності управлінських структур, у тому числі сил інформа ційної безпеки.

Стратегія навчання та вивчення дисципліни побудована на читанні лекцій, проведенні практичних (семінарських) занять із використанням активних форм навчання, а також проведенні « круглого столу» з проблемних питань інформаційної безпеки України. Проведенню підсумкового заняття може передувати обговорення письмових проектів з даної дисципліни.

НАВЧАЛЬНО-ТЕМАТИЧНИЙ ПЛАН ДИСЦИПЛІНИ «ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ЄВРОІНТЕГРАЦП»

№	Назва теми	Кількість годин			
		Лекції	Семінарські та практичні заняття	Самостійна та наукова рокота	Загалом
1.	Поняття та зміст інформаційної безпеки	2	2	2	6
2.	Національні інтереси України в інформаційній сфері	2	2	2	6
3.	Поняття та зміст загроз інформаційній безпеці	4	4	4	12
4.	Державна політика національної безпеки в інформаційній сфері	2	2	2	6
5.	Система забезпечення інформаційної безпеки	2	2	2	6
6.	Становлення інформаційного суспільства	4	4	2	10
7.	Інформаційна безпека України у сфері прав і свобод людини	2	2	2	6

8.	Інформаційна безпека Європей-ського Союзу	2	2	2	6
9.	Безпека інформа-ційного суспільства Європейського Союзу	2	2	2	5
10.	Адаптація стандартів Європейського Союзу Україною у сфері інформаційної безпеки	2	2	4	8
ІСПИТ					2
РАЗОМ		24	24	24	72

РОЗДІЛ 1 ПОНЯТТЯ ТА ЗМІСТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Вступ

Характерною ознакою сучасного етапу науково-технічного прогресу є стрімкий розвиток інформаційних технологій, їх використання як у повсякденному житті, так і в управлінні державою. Інформація та інформаційні технології все більше визначають розвиток суспільства і слугують новими джерелами національної могутності. Становлення інформаційного суспільства радикально змінює геополітичну обстановку в світі, впливає на формування нових сфер життєдіяльності людства, а відтак і національної безпеки. За цих умов формування інформаційного суспільства змінює предмет праці на інформацію і знання. У свою чергу, основою глобалізації стають інтеграція інформаційних систем різних держав до єдиної загальносвітової інформаційної системи, формування єдиного інформаційного простору, створення глобальних інформаційно-телекомунікаційних мереж, інтенсивне впровадження нових інформаційних технологій в усі галузі суспільного життя.

За ширмою цих, на поверхні позитивних процесів, стоять далеко на благочинні наміри створення світового уряду, обґрунтування концепції золотого мільярду, радикальне усунення космополітизму, концепція єдиного дому тощо.

Відтак, для усвідомлення розглядуваної проблематики, постає необхідність в окресленні поняття та змісту інформаційної безпеки як певної діяльності, спрямованої на створення достатніх умов для прогресивного розвитку національних інтересів в інформаційній сфері'. У більш широкому плані йдеться про:

- забезпечення інформаційного суверенітету України;

' *Ліпкан В А., Ліпкан О.С., Яковенко О.О. Національна і міжнародна безпека у визначеннях та поняттях. - К.: Текст, 2006. ~ С. 105.*

- удосконалення державного управління інформаційною сфе рою, впровадження інноваційних технологій у цій сфері, напов нення внутрішнього та світового інформаційного простору до стовірною інформацією про Україну;

активне залучення засобів масової інформації до боротьби з корупцією, організованою злочинністю, сепаратизмом, тероризмом та іншими формами екстремістської діяльності, зловживанням службовим становищем, іншими явищами, які створюють сприятливі умови або безпосередньо загрожують національній безпеці України,

- неухильне дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомір ного втручання системи органів державного управління їх по садових осіб у діяльність засобів масової інформації, дискримі нації в інформаційній сфері та переслідування журналістів за політичні позиції;

™ відповідальність ЗМІ за розповсюдження заздалегідь недос-товірної інформації;

- інформаційне виховання громадян України;

- вжиття комплексних заходів щодо захисту національного інформаційного простору, протидії монополізації інформаційної сфери України, встановлення контролю над нею з боку будь-яких недержавних чи транснаціональних корпорацій'.

Зазначимо, що розвиток інформаційних технологій є не лише важливою державною функцією, а й обов'язковою умовою забезпечення ефективного використання накопичених суспільством інформаційних ресурсів для створення розвиненого й убезпеченого інформаційного середовища. Цій меті слугує організація функціонування системи інформаційної безпеки, складовими компонентами якої є національні інтереси в інформаційній сфері, загрози цим інтересам, сама інформаційна безпека як інструмент зі створення сприятливих умов для їх реалізації, які

[2] *Ліпкан В А. Теоретичні основи та елементи національної безпеки України: Монографія. - К.: Текст, 2003. - С. 553.*

у сукупності становлять собою об'єкт управління органами державного управління, система забезпечення інформаційної безпеки, тобто суб'єкт управління, більше того, основні напрями політики національної безпеки в інформаційній сфері, а також внутрішнє та зовнішнє середовище. Зрозумілим є те, що інформаційна безпека забезпечується цілим комплексом заходів, відповідно їх вивченню приділяється певна наукова увага[1].

Осягнення сутності предмета, уяснення змісту **поняття «інформаційна безпека»** є важливим завданнями наукового аналізу. Будь-яке вчення лише тоді досягає зрілості та досконалості, коли розкриває сутність досліджуваних явищ, має можливість передбачати майбутні зміни не лише в сфері явищ, а й у сфері їх сутностеи. Пізнання сутності інформаційної безпеки можливо лише на основі абстрактного мислення, створення теорії досліджуваного предмета, уяснення внутрішнього змісту, виявлення характерних ознак.

В історичному процесі складається структура предмета, тобто єдність внутрішнього змісту та зовнішніх проявів, співпадаючих і неспівпадаючих суперечливих сутностеи. *Сутність* - сукупність глибинних зв'язків, відносин і внутрішніх законів, які визначають основні риси та тенденції розвитку системи. Сутність може вважатися пізнаною, коли є зрозумілими причини виникнення і джерела розвитку об'єкта, що розглядається, шляхи його формування або технічного репродукування, якщо в теорії або на практиці створена його достовірна модель. Одна й та сама сутність може мати множину різних явищ.

Сутність виражається і осягається в дефініції, що виражає родове поняття. Щодо інформаційної безпеки це є поняття національної безпеки, яке характеризує певний вид соціальної діяльності, основним змістом якої є створення сприятливих (необхідних і достатніх) умов для розвитку та реалізації національ-

[1] *Див. напр.: Кормич БЛ. Організаційно правові засади політики інформаційної безпеки України: Монографія. - Одеса: Юридична літера тура, 2003. -472 с*

 них інтересів[4]. Відповідно видове поняття «інформаційна безпека» різновид соціальної діяльності, який полягає в створенні державними і недержавними інституціями сприятливих умов для розвитку і реалізації національних інтересів в інформаційній сфері.

Інформаційна безпека є складовим компонентом загальної проблеми інформаційного забезпечення розвитку людини, держави і суспільства в якості симбіотичного організму. Вона орієнтована на захист значимих або вже згаданих суб'єктів інформаційних ресурсів, законних інтересів. Зміст поняття «інформаційна безпека» розкривається у практичній діяльності, наукових дослідженнях, а також нормативно-правових документах. Саме тому особливу увагу у даному розділі буде приділено класифікації підходів до визначення розглядуваного нами поняття.

1. Підходи до визначення поняття «національна безпека»

Національна безпека є складною неподільною системою, що саморозвивається, а отже складається з ряду підсистем (елементів) з відповідними чіткими взаємозв'язками як всередині системи, так із оточуючими її елементами, що у своїй сукупності утворюють нову якість. Серед інших ознак вищезгаданої системи слід також відзначити наявність відповідної структури, системної єдності та цілісності, зт^ялчної мети, відносної самостійності кожного окремого елемента системи з обов'язковим виконанням функцій, що необхідні для існування системи в цілому.

Серед вітчизняних науковців, що досліджують на достатньо серйозній методологічній основі проблеми національної безпеки,

[4] *Ліпкан ВА., Ліпкан О.С., Яковенко О.О. Національна і міжнародна безпека у визначеннях та поняттях. - К.: Текст, 2006. - С 146 - 147.*

можна відзначити таких: Горбулін В.П.[5], Нижник Н.Р., Ситник Г.П., Білоус В.Т.", ДанільянО.Г., Дзьобань О.П., Панов М.І.[7], Ліпкан В.АД Левицька М.Б.[9], Бодрук О.С.'", Гончаренко О.М., Лисицин Є.М. " та ін.

Так, О.М. Гончаренко, Є.М. Лисицин[12] вказують, що раніше ця категорія носила певною мірою абстрактний характер, а сьогодні нею оперують в практиці управління державою. Ок-

[5] *Горбулін В. П. Національна безпека України та міжнародна безпе ка І/ Політична думка. 1997.- № І. - С 76 - 89.*

[6] *Нижник Н.Р., Ситник Т.П., Білоус В.Т. Національна безпека Ук раїни (методологічні аспекти, стан і тенденції розвитку): Навчаль ний посібник І За заг. ред. П.В. Мельника, Н.Р.Нижник.-Ірпінь, 2000.- 304 с.*

[7] *Данільян О.Г., Дзьобань О.П., Панов М.І. Національна безпека України: сутність, структура та напрямки реалізації. - Харків: «ФОЛІО», 2002.-296 с*

[8] *Ліпкан В А. Національна безпека України: нормативно-правові ас пекти забезпечення. - К.: Текст, 2003. - 180 с; Ліпкан ВА. Теоретичні основи та елементи національної безпеки України: Монографія. - К.: «Текст», 2003. - 600 с; Ліпкан ВА. Теоретико-методологічні засади управління у сфері національної безпеки України: Монографія. - К.: Текст,2005. - 350 с*

[9] *Левицька М.Б. Теоретико-правові аспекти забезпечення націо нальної безпеки України органами внутрішніх справ України: Дис... канд...юрид. наук / 12.00.01 - К., 2002. - 206 с*

[10] *Бодрук О.О. Системи національної та міжнародної безпеки в умо вах формування нового світового порядку 1991-2001 роки : Дис. д-ра. політич. наук: 21.01.01./ Націон. ін-т проблем міжнар.безпеки. -К., 2003.-415 с*

" Гончаренко О.М., Лисицин Є.М. Методологічні засади розробки нової редакції концепції національної безпеки України . Національний інститут стратегічних досліджень Серія «Національна безпека», випуск 4,2001

[12] *Там само.*

В. А. ЛІПКАН, Ю. Є.МАКСИМЕНКО, В. М. ЖЕЛІХОВСЬКИИ, рім цього, розроблені та використовуються кількісні методики оцінки стану національної безпеки. За цими методиками, стан національної безпеки характеризується чисельною величиною, яка належить відрізку від нуля (найнижчий рівень стану національної безпеки, тобто найгірший її стан) до одиниці (найвищий рівень стану національної безпеки, тобто найкращий її стан). У зв'язку з чим, пропонують визначати національну безпеку як ступінь (міра, рівень) захищеності життєво важливих інтересів, прав і свобод особи, суспільства і держави від внутрішніх і зовнішніх загроз чи ступінь (міра, рівень) відсутності загроз правам і свободам людини, базовим інтересам та цінностям суспільства і держави.

У свою чергу, Данільян О.Г., Дзьобань О.П., Панов М.І. репрезентують поняття національної безпеки як стан захищеності життєво важливих інтересів особистості, суспільства і держави, людства в цілому від внутрішніх і зовнішніх загроз", яка стала класичною та була використана законодавцем у вищезгаданому Законі України «Про основи національної безпеки України».

Проведений авторами даного дослідження конвент-аналіз безпекових праць надав можливість говорити про існування певних підходів до визначення поняття «національна безпека».

Конструкція «стан захищеності (захисту)» при визначенні поняття «національна безпека» є найбільш поширеною. Хоча все більше дослідників наголошують, що таке визначення сформувалося в часи, коли «безпека» мала конкретне вираження, переважно в речах, і вимірювалася їх станом. Стан речей (матеріальних цінностей), їх властивостей був чітко визначений,

'■'• *Данільян О.Г., Дзьобань О.П., Панов М.І. Національна безпека України: сутність, структура та напрямки реалізації. - Харків: «ФОЛІО», 2002. - 296 с, С 9*

здебільшого не змінювався, а зміна зумовлювала новий сталий стан".

Вищезгадана конструкція справедливо критикується й через те, що віддзеркалює безпекознавчу парадигму, що існувала за радянських часів, коли пріоритет надавався захисту щодо попередження.

Нині, розкриття лише однієї сторони - захисту, при визначенні безпеки вважається неповним. Оскільки за такого розуміння принижується та втрачаються такі важливі властивості та функції безпеки як превентивні дії: звуження, послаблення, усунення і попередження небезпек та загроз. Зокрема, на дану обставину звертає увагу в своїй роботі російський дослідник Ярочкін В.І.".

Наявність загроз є атрибутом існування об'єкта будь-якої природи. Донедавна загрози вважалися не притаманними системі, негативними факторами. Внаслідок чого основною функцією суб'єктів забезпечення безпеки була цілковита їх ліквідація. Неможливість цього сприяло зміні розуміння цієї функції з ліквідації на управління загрозами з метою мінімізації негативного, деструктивного впливу щодо функціонування та життєдіяльності об'єктів забезпечення безпеки.

Деякі дослідники говорять не тільки про іманентний характер загроз, але й відзначають їх творчо-конструктивну роль у розвитку об'єкта. Зокрема, дана позиція репрезентована у роботі В.А.Ліпкана «Безпекознавство»[6].

Отже, національна безпека розглядається в якості інтегративної сукупності різних сфер життєдіяльності суспільства, однією з яких є інформаційна сфера.

" Гурковський В.І. Організаційно правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: Дис... канд... юрид. наук \ 25.00.02 - К.. 2004. - 225 с. , С 32

[15] Ярочкин В.И. Секьюритология - наука о безопасности жизнедеятельности. - М.: «Ось-89»,2000. - 400 с, С 213

"' Ліпкан ВА. Безпекознавство: Навч. посібник.-К.: Вид-во Європ. ун-ту, 2003- 208 с. С. 35

Поняття інформаційної сфери

Особливістю розвитку сучасного суспільства є збільшення ролі інформаційної сфери в житті людини, а відповідно й інформаційної діяльності. Так, згідно зі ст. 12 Закону України «Про інформацію» від 2 жовтня 1992 р., «інформаційна діяльність -це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави». Основні напрямки інформаційної діяльності: політичний, економічний, соціальний, духовний, екологічний, науково-технічний, міжнародний тощо. Основні види інформаційної діяльності: отримання, використання, поширення та зберігання інформації. На сьогодні в національному законодавстві не легалізовано поняття «інформаційна сфера». Вважаємо, що нині як на побутовому, так і на науковому рівні інформаційна сфера розглядається як така, що формується та розвивається під час інформаційної діяльності.

На сьогодні інформаційна сфера розглядається і як відносно самостійна сфера, і як допоміжна стосовно інших видів діяльності. В останньому випадку йдеться про те, що інформаційна сфера обслуговує практично всі аспекти суспільного життя (економіку, політику, управління, науку, культуру, побут, сім'ю), тобто займає підлегле положення.

Як у першому, так і в другому випадку мається на увазі вузьке тлумачення поняття «інформаційна сфера». Існуюча політика держави в інформаційній сфері спрямована як на її розвиток безпосередньо, так і на підвищення з її допомогою ефективності розвитку державності, безпеки, оборони, пріоритетних галузей економіки, фінансової та грошової системи, соціальної сфери, галузей екології та використання природних ресурсів, науки, освіти та культури, міжнародного співробітництва. Багато уваги приділяється підвищенню ефективності державного управління як одній з пріоритетних функцій держави. Це підтверджується Концепцією Національної програми інформатизації, в якій ін-

форматизація розглядається як важливий засіб розвитку України, та Указом Президента України «Про заходи щодо забезпечення інформаційної безпеки держави» від 18 вересня 2002 р.

Варто підкреслити, що відповідна державна політика проводиться і щодо підтримки розвитку даної сфери, а саме: ЗМІ, науково-технічної інформації, видавничої справи та реклами, статистики, бібліотечної та архівної справи, інформатики та обчислювальної техніки тощо. У такому вигляді ця політика легалізована та легітимізована у законах України: «Про Національну програму інформатизації», «Про Концепцію Національної програми інформатизації», «Про інформацію» тощо.

У нових умовах становлення та розвитку інформаційного суспільства інформація та новітні інформаційно-комунікаційні технології стають його головною рушійною силою. Слід зазначити, що відповідно до Закону України «Про Національну програму інформатизації» *«інформаційний продукт (продукція)* - це документована інформація, яка підготовлена та призначена для задоволення потреб користувачів».

В умовах інформаційного суспільства починає змінюватися не тільки рівень автоматизації виробництва, а й саме виробництво - продукт його стає більш ємним, що означає збільшення частки інновацій, дизайну і маркетингу в його вартості. Виробництво інформаційного, а не матеріального продукту визначає інформаційне суспільство. Знання стає головним стратегічним ресурсом такого суспільства, інформація проникає в усі сфери суспільства та держави. Йдеться про те, що коригується поняття «інформаційна сфера». Ці процеси активно відбуваються у інформаційно розвинених державах світу, зокрема у країнах Європейського Союзу.

На сьогодні інформаційна сфера системостворюючий чинник життя суспільства та держави, вона активно впливає на політичну, економічну, воєнну та інші складові національної безпеки країни, а у багатьох країнах і «вбирає» їх.

3. Співвідношення понять національної та інформаційної безпеки

Дослідники національнобезпекової проблематики виділяють чимало складових, що становлять сутнісне наповнення національної безпеки. Однією з них є інформаційна складова.

Дискусійним залишається питання: чи є інформаційна безпека складовою національної, чи необхідно, зважаючи на неподільність та цілісність національної безпеки, казати про національну безпеку в інформаційній сфері, відтак розглядати прояви національної безпеки у цій сфері.

У ст. 17 Конституції України закріплено, що захист суверенітету та територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу'[7].

У Законі України «Про основи національної безпеки України» від 19 червня 2003 р.'[я] йдеться «про основні сфери національної безпеки» , серед яких виокремлюється й інформаційна.

У концептуальному плані вважається, що національна безпека становить собою цілісний екзистенціальний феномен, відтак не може бути репрезентована сукупністю корелятивно пов'язаних складових (економічна, інформаційна, політична безпека тощо). Національну безпеку слід аналізувати крізь призму її системних властивостей, отже доцільно казати про національну безпеку в інформаційній сфері, екологічній та ін. Адже із появою інших «складових» національна безпека як така не змінить своєї сутності. Водночас, коли йтиметься про прояви національної безпеки у різних сферах життєдіяльності, то поява чи то нових суспільних відносин, чи то сфер життєдіяльності жодним чином не вплине на зміст національної безпеки, лише змінить її

[17] Конституція України // Відомості Верховної Ради (ВВР). - 1996. - № ЗО.-Ст. 141.

[14] Прооснови національноїбе.теки України: Закон України // Офіційний Вісник України. - 2003. - № 29. - Ст. 1433

форму, оскільки національна безпеки знаходитиме свій прояв в нових сферах.

Органічна ж сукупність елементів, що входять до націо-безпекового середовища, поєднані між собою кореляційними зв'язками, утворюють систему національної безпеки. Саме у цьому полягає основні відхилення наукових досліджень безпе-кової проблематики, котрі при дослідженні даного феномену не використовують евристичний потенціал націобезпекознавчого підходу.

Інтегруючи положення щодо розглядуваного питання, викладемо основні постулати *авторського* бачення даної проблеми.

1. Національні інтереси, загрози їм, управління цими загрозами в усіх галузях національної безпеки знаходять свій вираз, реалізуються через інформацію та інформаційну сферу.

2. Людина та її права, інформація та інформаційні системи та права на них - це основні об'єкти не лише національної безпеки в інформаційній сфері, але й основні елементи всіх об'єктів безпеки в усіх галузях.

3. Розв'язання завдань національної безпеки пов'язано з використанням інформаційного підходу як основного науково-практичного методу.

4. Проблема національної безпеки має яскраво виражений ін-формаційний характер[9].

5. Нехтування розвитком інформаційної сфери унеможливлює забезпечення національної безпеки.

6. Інформаційна складова є притаманною будь-якій сфері життєдіяльності.

4. Підходи до визначення поняття «інформаційна безпека»

[19] *Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство /Санкт-Петербургский университет МВД России.- СПб.:Фонд «Университет», 2000.- 428 с, С. 73*

Такі поняття, як інформаційна безпека, інформаційний суверенітет, інформаційний простір та поняття, що пов'язані з даною проблематикою, є досить популярними та, на перший погляд, зрозумілими. Втім, не можна оминути той факт, що вони є доволі дискусійними в наукових колах, через що досі не знайшли свого уконституювання у відповідних законодавчих актах.

Продуктивним є методологічний підхід до дослідження джерел з національної безпекової тематики, зроблений Ліпканом В.А., який виокремлює три групи визначення поняття «національна безпека», а саме: нормативно-правова (в основі лежить аналіз нормативно-правових актів, які містять дефініцію певних видів безпеки), доктринальна (в основі - аналіз визначень в роботах науковців, дослідників даної проблематики), енциклопедична (аналіз визначень, що містять словники, енциклопедії)[20].

Незважаючи на актуальність інформаційної складової національної безпеки України, на сьогодні в законодавстві відсутня норма, яка б містила дефініцію поняття «інформаційна безпека», враховуючи різницю між інформаційною безпекою та безпекою інформації. Для всебічного, повного розгляду поняття «інформаційна безпека» та, використовуючи запропонований Ліпканом В.А. алгоритм дослідження базового поняття, зупинимось на кожній з груп.

4.1. Нормативно-праеоеа група

Закон України «Про основи національної безпеки України» від 19 червня 2003р. та інші нормативно-правові акти, спрямовані на регулювання суспільних відносин в інформаційній сфері, практично нормативно не закріплюють вищезазначених понять.

Даний тезис підтверджується нормами єдиного нормативно-правового акту, в якому здійснено спробу щодо окреслення загальних підходів до окреслення сутності даного феномену,

[20] *Ліпкан ВЛ. Теоретичні основи та елементи національної безпеки України: Монографія.- К.: «Текст», 2003.-600 е., С.415*

Законом України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 року.

Відповідно до даного документу *інформаційна безпека* є невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки. *Об'єктами інформаційної безпеки* є інформаційні ресурси, канали інформаційного обміну та телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни. Результатом виконання Програми мав би стати пакет нормативних документів з усіх аспектів використання засобів обчислювальної техніки для оброблення та зберігання інформації обмеженого доступу; комплекс державних стандартів із документування, супроводження, використання, сертифікаційних випробувань програмних засобів захисту інформації; банк засобів діагностики, локалізації і профілактики вірусів, нові технології захисту інформації з використанням спектральних методів, високо надійні криптографічні методи захисту інформації тощо[21].

У Законі України «Про основи національної безпеки України» поняття «інформаційна безпека» не знаходить свою опера-ціоналізацію, втім зазначається на інформаційну сферу національної безпеки, при чому, не дається визначення навіть і даного поняття, а лише перераховуються загрози та напрями державної політики у вищезазначеній сфері.

Перелік загроз, визначений законодавцем в цьому законі, дає можливість стверджувати про розуміння інформаційної безпеки, не як безпеки інформації в технічному аспекті, а більш широку категорію, що дещо суперечить розумінню інформаційної безпеки у Законі України «Про Концепцію Національної програми інформатизації».

4.2. Енциклопедична група

[21] Закон України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 року \\ Відомості Верховної Ради . - 1998. - № 27-28.-Ст.. 182.

В. А. ЛІПКАН, Ю. Є.МАКСИМЕНКО, В. М. ЖЕЛІХОВСЬКИЙ
Енциклопедична група представлена першою в Україні багатотомною юридичною енциклопедією, в другому томі якої (виданому в 1999 році) і є спроба дати визначення інформаційної безпеки. Водночас зазначимо, що в Українській радянській енциклопедії та в інших радянських енциклопедіях не міститься цікавих для розкриття сутності феномену «інформаційної безпеки» визначень.

Отже, *інформаційна безпека України* - один із видів національної безпеки, важлива функція держави. Інформаційна безпека України означає:

- законодавче формування державної інформаційної політики;
- створення відповідно до законів України можливостей досягнення інформаційної достатності для ухвалення рішень органами державної влади, громадянами та об'єднаннями громадян, іншими суб'єктами права в Україні;
- гарантування свободи інформаційної діяльності та права доступу до інформації у національному інформаційному просторі України;
- всебічний розвиток інформаційної структури;
- підтримка розвитку національних інформаційних ресурсів України з урахуванням досягнень науки та техніки й особливостей духовно-культурного життя народу України;
- створення і впровадження безпечних інформаційних технологій;
- захист права власності держави на стратегічні об'єкти інформаційної інфраструктури України;
- охорону державної таємниці, а також інформації з обмеженим доступом, що є об'єктом права власності або об'єктом лише володіння, користування чи розпорядження державою;
- створення загальної системи охорони інформації, зокрема охорони державної таємниці, а також іншої інформації з обмеженим доступом;

- захист національного інформаційного простору України від розповсюдження спотвореної або забороненої для поширення за конодавством України інформаційної продукції;
- встановлення законодавством режиму доступу іноземних держав або їх представників до національних інформаційних ре сурсів на основі договорів з іноземними державами;
- законодавче визначення порядку поширення інформаційної продукції зарубіжного виробництва на території України".

4.3. Доктринальна група

Розуміючи строкатість визначень, що можуть бути включені для аналізу в доктринальну групу, ми, використовуючи порівняльний метод, а також методи івент-аналізу та контент-аналі-зу, керувались при виборі як принципом розповсюдженості та популярності обігу в наукових колах, так і рівнем зацікавленості та досліджуваності (кількість наукових праць, дисертаційних досліджень тощо) феномену інформаційної безпеки нижчезазна-чених авторів.

Виходячи з найбільш імовірних загроз національній безпеці України в життєво важливих сферах діяльності, *Нижник Н.Р., Ситник Г.П., Білоус В.Т.*[23], виокремлюють ряд основних функціональних складових (сфер) національної безпеки України: економічну, політичну, соціальну, воєнну, екологічну, епідемічну, технологічну та інформаційну безпеку.

Зокрема, під *інформаційною безпекою,* вищеназвані автори розуміють стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для прийняття стратегічних рішень та захист інформаційних ресурсів країни.

[22] *Юридична енциклопедія: В 6 т. / Редкол.: Ю.С. Шемшученко (відп. ред.) та ін. - К.: Укр. енцик., 1998. - 1999. - Т. 2.: Д - Й. - 744 с.;С. 714*

[23] *Нижник Н.Р., Ситник Г.П., Білоус В.Т. Національна безпека Ук раїни (методологічні аспекти, стан і тенденції розвитку): Навчаль ний посібник І За заг. ред. П.В. Мельника, Н\Р'.Нижник. - Ірпінь, 2000.- 304 с, С 54*

Зацікавленість викликає робота таких дослідників як *Дані-льян О.Г., Дзьобань О.П., Панов М.І.,* які у своєму навчальному посібнику *«Національна безпека України: сутність, структура та напрямки реалізації»*[24], визначають інформаційну безпеку як безпеку об'єкта від інформаційних загроз або негативних впливів, пов'язаних з інформацією та нерозголошення даних про той чи інший об'єкт, що є державною таємницею.

Вони також акцентують увагу на проблемі інформаційних війн, оскільки на сьогодні вона становить собою ефективний і цивілізований шлях колонізації однієї країни іншою та виділяють крім цього такі загрози інформаційній безпеці як розголошення інформації, яка становить державну таємницю, вплив засобів масової інформації на свідомість людини та суспільства, забезпечення державних організацій повною, достовірною і своєчасною інформацією, що необхідна для прийняття рішень, неінтегрованість України до світового інформаційного поля, недостатня кваліфікованість та активність українських інформаційних служб, використання інформаційних технологій кримі-налітетом тощо.

Дитвиненко О.В.[25] під інформаційної безпекою розуміє єдність трьох складових: забезпечення захисту інформації; захисту та контролю національного інформаційного простору; забезпечення належного рівня інформаційної достатності.

Цікавим та водночас дискусійним є визначення *Кормича БА.,* який зазначає, що *інформаційна безпека* - це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією

[24] *Данільян О.Г., Дзьобань О.П., Панов М.І. Національна безпека України: сутність, структура та напрямки реалізації. - Харків: «ФОЛІО», 2002. - 296 с*

[25] *Литвиненко О.В. Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії): Автореф. дис.... канд. політ, наук . 23.00.04. - К., 1997 - 18 с*

умови існування і розвитку людини, всього суспільства та держави-[6].

Російський вчений *Лопатін В.М.* визначає інформаційну безпеку як стан захищеності національних інтересів країни (життєво важливих інтересів особи, суспільства та держави на збалансованій основі) в інформаційній сфері від внутрішніх та зовнішніх загроз-[7], що віддзеркалює норму права Закону РФ «О безопасности», згідно з яким «Безопасность - состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз»[г]*.

Використовує категорію національних інтересів і Баранов 0., відповідно визначаючи інформаційну безпеку як стан захищеності національних інтересів України в інформаційному середовищі, за якого не допускається (або зводиться до мінімуму) завдання шкоди особі, суспільству, державі через неповноту, несвоєчасність, недостовірність інформації й несанкціоноване її поширення та використання, а також через негативний інформаційний вплив та негативні наслідки функціонування інформаційних технологій[29].

Акцент на такій складовій інформаційної безпеки як безпека інформації, знаходить свій вираз також у визначеннях інших дослідників цієї проблематики, наприклад, інформаційна безпека ^ це стан захищеності інформаційного простору, що

[26] *Кормич БА. Організаційно-правові засади політики інформацій ної безпеки України: Монографія.- Одеса: Юридична література, 2003-- 472 с, С 142*

[27] *Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство,/Санкт-Петербургский университет МВД России,- СПб.:Фонд «Университет», 2000.- 428 с,, С. 79*

[28] *О безопасности: Закон Российской Федерации // Ведомости Вер ховного Сонета РФ. - 1992. - № 15. - Ст. 770*

[29] *Баранов А. Информационный суверенитет или информационная безопасность ? // Нац. безпека і оборона. - 2001. - № 1(13). - С.70-76., С. 72*

забезпечує його формування та розвиток в інтересах громадян, організацій та держави, стан інфраструктури системи (об'єкта, держави), при якому інформація використовується суворо за призначенням та не завдає негативного впливу на систему (об'єкт, державу) при її використанні; стан інформації, за якого виключається чи суттєво ускладнюється порушення таких її властивостей як таємність, цілісність та доступність [30].

Неординарністю та інноваційністю відрізняється також й визначення *Гурковського В.І.,* відповідно до якого національна інформаційна безпека України - це суспільні відносини, пов'язані із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі, що є необхідною умовою збереження та примноження духовних і матеріальних цінностей державоутво-рюючої нації, її існування, самозбереження і прогресивного розвитку України як суверенної держави, що залежить від цілеспрямованої інформаційної політики гарантій, охорони, оборони, захисту її національних інтересів[31].

На думку *Ярочкіна В.І. та Шевцової ТА.,* інформаційна безпека - це проведення правових, організаційних та інженерно-технічних заходів при формуванні та використанні інформаційних технологій, інфраструктури та інформаційних ресурсів, захисті інформації високого значення й прав суб'єктів, що беруть участь в інформаційній діяльності[32]. У даному визначенні інформаційна безпека зводиться до захисту інформації, що не зовсім відбиває її сутність.

[30] *Крутских А., Федоров А. О междунароной информационной безо пасности II Международная Жизнь. - 2000. - № 2. - С.43-47, С. 44*

[31] *Гурковський ВТ. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: Дис... канд... юрид. наук \ 25.00.02 - К., 2004. - 225 с, С 35*

[32] *Ярочкин В.И., Шевцова ТА. Словарь терминов и определений по безопасности и защите информации.- М.: «Ось-89», 1996.- 78 с, С. 8*

Харчелко Л.С., Ліпкан В А., Логінов О.В. визначили, що інформаційна безпека - це складова національної безпеки, процес управління загрозами та небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України[33].

При чому, сам В.А.Єліпкан акцентував увагу на тій обставині, що родове поняття, а звідти й видові, мають визначатися крізь діяльнісну формулу процесу. Це зумовлено тією обставиною, що процес відрізняється від поняття стан. Поняття процес означає послідовність станів, пов'язаність стадій їх зміни і розвитку, тобто на відміну від поняття «стан», поняття «процес» акцентує увагу на моменті спрямованості в зміні об'єкту, цілепокладанні. У той час, як «стан» відображає лише один момент, певну мить безпеки, а отже не вичерпує її повністю.

Таким чином, визначаючи поняття інформаційної безпеки, можна виокремити декілька підходів окреслення сутності цього феномену, а саме розуміння інформаційної безпеки в якості:

1. Стану захищеності інформаційного простору.
2. Процесу управління загрозами та небезпеками, що забезпечує інформаційний суверенітет України.
3. Стану захищеності національних інтересів України в інформаційному середовищі.
4. Захищеності встановлених законом правил, за якими відбуваються інформаційні процеси в державі.
5. Вжиття певних заходів.
6. Стану захищеності національних інтересів країни в інформаційній сфері.
7. До суспільних відносин, пов'язаних із захистом життєво важливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі.

[33] *Харченко Л.С., Ліпкан В А., Логінов О.В.Інформаційна безпека України: Глосарій І За загальною редакцією доктора юридичних наук, професора РА.Калюжного.- К.: «Текст», 2004.-180 с, С. 47*

8. Важливої функції держави.

9. Невід'ємної частини політичної, економічної, оборонної та інших складових національної безпеки.

Строкатість поглядів на визначення поняття «інформаційна безпека» є зрозумілою, оскільки, як вірно зазначають *Нижник Н.Р., Ситник Г.П., Білоус В.Т.,* до цього часу бракує єдиної думки в трактуванні базових понять національної безпеки, що дає теорія, яка передбачає:

- формування базових понять (створення відповідного по нятійно-категоріального апарату);
- встановлення їх структурно-функціональних зв'язків;
- вибір підходу (підходів) до формалізації процесів, що аналізуються (вивчаються), та розробка на цій основі методів дослідження, які б забезпечили поглиблене вивчення та виявлення ВІДПОВІДНРІХ (властивих даному об'єкту досліджень) закономірностей[3]*.

Данільян О.Г., Дзьобань О.П., Панов М.І. стверджують, що це пов'язано як з певним суб'єктивізмом дослідника, який використовує вироблені наукою та філософією сукупність понять і категорій, інтерпретуючи їх у властивий для себе спосіб, так і з взагалі з переглядом багатьох традиційних положень, формуванням принципово нових концепцій, введенням в науковий обіг нових понять і категорій[35].

Отже, конструктивним шляхом щодо визначення поняття «інформаційна безпека», є виокремлення його базових ознак, яке є похідним від поняття національна безпека, і має враховувати його сутнісні ознаки.

[34] *Нижник Н.Р., Ситник Г.П., Білоус В.Т. Національна безпека Ук раїни (методологічні аспекти, стан і тенденції розвитку): Навчаль ний посібник І За заг.ред. П.В. Мельника, Н.Р.Нижник.-Ірпінь, 2000-304с.,С12*

[35] *Данільян ОТ., Дзьобань О.П., Панов М.І. Національна безпека України: сутність, структура та напрямки реалізації. - Харків: «ФОЛІО», 2002.-296 с.,С68*

Даний підхід більш детально розписаний у монографії В.А.Ліпкана «Теоретико-методологічні засади управління у сфері національної безпеки України»[36]. Методологічні ж проблеми, які спіткають дослідників феномену національної безпеки і її проявів в різних сферах життєдіяльності, викладені у монографії В.А.Ліпкана «Теоретичні основи та елементи національної безпеки України», в якій робиться спроба щодо формування теорії національної безпеки - націобезпекознавства. За задумом автора воно має виступати теоріостворюючим гносеологічним елементом загальної будови системи знань про національну безпеку.

Висновки

Отже, *інформаційна безпека* являє собою одне з важливіших понять у науці та різних сферах людської діяльності. Сутність і комплексність цього поняття виявляється характером сучасного інформаційного суспільства. Аналіз різних підходів до визначення змісту поняття «інформаційна безпека» уможливлює зауважити про недоцільність суворого обрання тієї чи іншої позиції. Наведені вище погляди, а вірніше сказати підходи до визначення поняття інформаційної безпеки дають змогу розглядати дану проблему більш комплексно і системно, додати знань про цей багатогранний феномен. Більше того, на наше переконання, найбільш прийнятним є інтегральний підхід, за якого інформаційна безпека визначатиметься за допомогою окреслення найбільш важливих її сутнісних ознак з урахуванням постійної динаміки інформаційних систем і становлення не лише інформаційного суспільства а й інформаційної цивілізації.

Такий підхід уможливив дійти висновку, що інформаційна безпека не може розглядатися лише в якості окремого стану.

[36] *Ліпкан ВЛ. Теоретико-методологічні засади управління у сфері національної безпеки України: Монографія. - К.: Текст, 2005. - С. 210 - 213.*

Безперечно, що це є і властивістю, атрибутом інформаційного суспільства, діяльністю і результатом діяльності людини, спрямованої на забезпечення певного рівня безпеки в інформаційній сфері. Інформаційна безпека має враховувати майбутнє, а отже вона не є станом, а становить собою процес. Таким чином, інформаційну безпеку слід розглядати крізь органічну єдність ознак, таких як стан, властивість, а також управління загрозами і небезпеками, за якого забезпечується обрання оптимального шляху їх усунення і мінімізації впливу негативних наслідків, що врешті-решт за своїм змістом і становить діяльність по створенню сприятливих умов для реалізації інтересів об'єкта.

Інформаційна безпека за своєї суттю є більш широким, ніж захист інформації, поняттям. Отже інформаційна безпека - багатогранна сфера діяльності, для усвідомлення сутності якої успіх може принести системно-комплексний підхід.

Дослідження сутності інформаційної безпеки має враховувати той факт, що сутність є внутрішнім змістом предмету, який знаходить вираз у стійкій єдності усіх багатоманітних і суперечливих формах буття. Базовою характеристикою інформаційної безпеки слід вважати імовірність появи загрози підвищеного ризику реалізації загрози або небезпеки для індивіда, суспільства та держави. Критерієм ефективності забезпечення інформаційної безпеки є високий рівень безпеки при мінімумі відповідних затрат. Отже можна говорити про структуру поняття інформаційної безпеки. Основним її елементом є життєво важливі інтереси соціальної системи, які співвідносяться із зовнішніми чинниками у вигляді інтересів наднаціональних або інших національно-державних структур в рамках міжнародного співтовариства. Зсередини національно-державного утворення його життєво важливі інтереси перебувають у взаємодії з інтересами елементів, які складають дане утворення. В якості останніх виступають соціальні групи, еліта, організації, партії, релігійні та етнічні утворення, рухи тощо. Сукупність внутрішніх і зовнішніх інформаційних загроз

створюють передумови для порушення безпечного функціонування системи державного управління.

Вагомість інформаційно-комунікаційних процесів у сучасному світі дає підстави розглядати забезпечення інформаційної безпеки як одне з глобальних і пріоритетних завдань органів державного управління, вирішенню якого мають бути підпорядковані політична, економічна, воєнна, культурна та інші види діяльності системи державного управління.

Національні інтереси в інформаційній сфері є похідними від національних цінностей. Отже, інтереси інформаційної безпеки випливають із таких цінностей, як права людини, свобода, економічне процвітання, могутність країни. Саме тому головним інтересом для України є її виживання як вільної, незалежної нації при збереженні фундаментальних цінностей та інститутів безпеки. Одним з механізмів гарантування даного процесу є ефективно функціонуюча система державного управління, яка є суб'єктом і об'єктом забезпечення інформаційної безпеки одночасно. І у даному випадку намагання багатьох країн забезпечити власну інформаційну безпеку за рахунок інших країн викликають з одного боку, занепокоєння, а з іншого - упевненість у необхідності формування дієздатної системи забезпечення інформаційної безпеки органів державного управління.

Інформаційна безпека виступає як характеристика стабільного, стійкого стану системи державного управління, яка при впливі внутрішніх та зовнішніх загроз та небезпек зберігає суттєво важливі характеристики для власного існування.

Інформаційна безпека як одна з характеристик стійкого розвитку виступає в якості базової цінності держави. У той же час, ціннісні орієнтації, що ґрунтуються на уявленнях про інформаційну безпеку в різних соціальних груп і окремих осіб, почасти не співпадають. Саме у цьому знаходить свій безпосередній вираз вплив держави, яка за допомогою значного арсеналу методів виражає і забезпечує реалізацію спільних цінностей особи, суспільства та держави в інформаційній сфері.

національна безпека, інформаційна сфера національної безпеки, інформаційна складова національної безпеки, інформаційна безпека

Контрольні запитання для самоперевірки

1. Які основні підходи до визначення поняття «інформаційна безпека» ви знаєте?

2. Назвіть основні ознаки інформаційної безпеки?

3. У якому документі нормативно закріплена дефініція інформаційної безпеки?

4. Назвіть основні причини строкатості визначення поняття «інформаційна безпека»?

5. Розкрийте зв'язок між національною та інформаційною безпекою ?

Завдання для самопідготовки

1. Сформуйте власну модель формування поняття інформаційна безпека.

2. Окресліть детермінантний вплив концепції безпеки на визначення поняття «інформаційна безпека».

Список рекомендованої літератури

Нормативні джерела

1. *Конституція* України // Відомості Верховної Ради (ВВР). -1996. ~№30. -Ст. 141.

2. *Про вдосконалення* державного управління інформаційною сферою: Указ Президента України від 16 вересня 1998 р. // Голос України. - 1998. - № 182.

3. *Про Концепцію* Національної програми інформатизації Закон України від 4 лютого 1998 року.

4. *Про основи* національної безпеки України: Закон України // Офіційний Вісник України. - 2003. - № 29. - Ст. 1433.

Доктринальні джерела

1. *Актуальні* проблеми інформаційної безпеки України: аналіт. доп. УЦЕПД) // Нац. безпека і оборона. - 2001. - №1 (13). -С.2-50.

2. *Баранов А.* Информационный суверенитет или информационная безопасность? // Нац. безпека і оборона. - 2001. - № 1(13). -С. 70-76.

3. *Білорус О. Г.* Глобалізація і національна стратегія України. Броди: Просвіта, 2001. - 299 с

4. *Білорус О. Г.* Глобалізація і безпека розвитку / [Білорус О. Г., Гончаренко М. О., Зленко В. А. та ін.]; НАН України, Київ, нац. екон. ун-т. - К.: КНЕУ, 2001. - 733 с

5. *Бодрук О.О.* Системи національної та міжнародної безпеки в умовах формування нового світового порядку 1991-2001 роки: Дис. д-ра. політич. наук: 21.01.01./ Націон. ін-т проблем між-нар.безпеки. - К., 2003.- 415 с

6. *Голубев В. О., Гавловський В. Д., Цимбалюк В. С.* Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / За заг. ред. Р.А. Калюжного, М.Я. Швеця . - Запоріжжя : Просвіта, 2001. - 252 с

7. *Гончаренко О.М., Лисицын Є.М.* Методологічні засади розробки нової редакції концепції національної безпеки Украї ни: Нац. ін-т стратег, досл. Серія «Національна безпека», випуск 4,2001.

8. *Горбулін В. П.* Національна безпека України та міжнародна безпека // Політична думка.- 1997.- № 1.- С. 76 - 89.

9. *Гурковський В. І.* Інформаційна безпека в Україні як складова національної безпеки // 36. наук. пр. УАДУ - 2002. - № 2. -С. 9-18.

10. *Гурковський В.І.* Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: Дис.канд... юрид. наук \ 25.00.02 - К., 2004. - 225 с

11. *Данільян О.Г., Дзьобань О.П., Панов М.І.* Національна безпека України: сутність, структура та напрямки реалізації.
- Харків: «ФОЛІО», 2002. - 296 с

12. *Кормич БА.* Організаційно-правові засади політики інформаційної безпеки України: Монографія.- Одеса: Юридична література, 2003.- 472 с

13. *Крушених А., Федоров А.* О междунароной информационной безопасности // Международная Жизнь. - 2000. - № 2. - С. 43-47

14. *Литвиненко О.В.* Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії): Автореф. дис. ... канд. політ, наук . 23.00.04. - К., 1997 -18 с.

15. *Ліпкан ВА.* Теоретико-методологічні засади управління у сфері національної безпеки України: Монографія. - К.: Текст, **2005.-350** с

16. *Ліпкан ВА.* Теоретичні основи та елементи національної безпеки України: Монографія. - К.: «Текст», 2003. - 600 с

17. *Ліпкан ВА., Ліпкан О.С., Яковенко О.О.* Національна і міжнародна безпека у визначеннях та поняттях. - К.: Текст, 2006.-256 с

18. *Логінов О.В.* Сучасні проблеми забезпечення інформацій ної безпеки в контексті формування системи державного управ ління // Науковий вісник Юридичної академії МВС України.
- **2003.** - № 3. - С **199-205.**

19. *Лопатин В.Н.* Информационная безопасность России: Че ловек. Общество. Государство./Санкт-Петербургский универси тет МВД России.- СПб.-.Фонд «Университет», 2000. - 428 с.

20. *Нижник Н.Р., Ситник Г.П., Білоус В.Т.* Національна безпека України (методологічні аспекти, стан і тенденції роз-

витку): Навчальний посібник / За заг. ред. П.В. Мельника, Н.Р.Нижник.-Ірпінь, 2000.- 304 с

21. *Павлютенкова М.* Информационная война - реальная уг роза или современный миф? // Власть. - 2001. - № 12. - С. 19 - 23.

22. *ПочепцовГ.Г.* Информационные войны / С.Л. Удовик(отв. ред.). - М.: Рефл-бук, 2000. - 576 с.

23. *Харченко Л.С., Ліпкаи ВЛ., Логінов О.В.* Інформаційна безпека України: Глосарій. - К.: Текст, 2004. - 136 с.

24. Юридична енциклопедія: В 6 т. / Редкол.: Ю.С. Шемшу-ченко (відп. ред.) та ін. - К.: Укр. енцик., 1998. - 1999. - Т. 2.: Д-Й.-744 с.

25. *Ярочкин В.И., Шевцова ТА.* Словарь терминов и определений по безопасности и защите информации.- М.: «Ось-89», 1996. - 78 с.

В. А. ЛШКАН, Ю. Є.МАКСИМЕНКО, В. М. ЖЕЛІХОВСЬКИИ

РОЗДІЛ 2
НАЦІОНАЛЬНІ ІНТЕРЕСИ УКРАЇНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Вступ

Категорія «національні інтереси» являє собою першооснову побудови системи національної безпеки. Відтак визначенню національних інтересів в інформаційній сфері має передувати загальний аналіз даної категорії, необхідності і застосування, підходів до визначення та механізмів формування.

Серед науковців, які досліджують проблему національних інтересів можна виділити таких як: В. Горбулін, О. Белов, Б. Па-рахонський, С. Пирожков, В. Косєвцов, І. Бінько, В. Косола-пов, А. Гірник, О. Матвієвський, О. Гончаренко, В. Соломатова, І.Кресіна тощо.

У науковому колі дискусійним залишається питання співвідношення понять «національна безпека» та «національні інтереси», а тому дещо зупинимось на цьому питанні.

Чимало дослідників акцентують увагу на проблемі широкого трактування категорій «національна безпека» та «національні інтереси», що фактично призводить до підміни іншої категорії, наприклад, «функція держави», а також злиття їх предметів. Найбільш популярною та логічною, є розуміння того, що національні інтереси є категорією більш широкою, ніж національна безпека. У свою чергу, національна безпека є не лише інструментом задоволення національних інтересів, а й одним з життєво важливих національних інтересів. Безпечні умови існування людини та суспільства, функціонування державно-правових інституцій є основою, плацдармом для їх подальшого розвитку та задоволення інших потреб.

Виникає закономірне питання: чим же визначаються ці національні інтереси, на що спрямована їхня реалізація? Звичайно, що відповідь на дане питання має багатовимірну природу. Не

можна не сказати, що чим більше за територією держава, тим глобальнішими є її національні інтереси. Без сумніву національні інтереси королівства Монако, є на порядок вужчими, ніж національні інтереси Туреччини, у той же час національні інтереси останньої є вужчими за національні інтереси Китаю. Взагалі ж на формування національних інтересів впливають чинники абсолютно різної природи, через що розгляд даного питання потребує окремих самостійних досліджень. Нас же у цьому плані, відповідно до мети дослідження, цікавлять чинники, що впливають на формування національних інтересів України.

Україна - велика європейська держава, яка має територію 603,7 тис. км^2 та населення близько 45 млн. Кліматичні умови країни сприяють розвитку як сільського, так і лісового господарства.

Україна розташована у самому центрі Європи, і усілякі концепції щодо віднесення її або до західної частини Євразії, або до східної частини Європи є нічим іншим як застосування засобів інформаційного впливу на формування спотвореного образу нашої держави.

Україна - центр Європи, саме тому її роль у побудові європейської спільноти є вагомою, а згодом і визначальною. Перебуваючи на перетині цивілізацій, Україна є уособленням інтеграції різних культур, а отже і продуцентом інтегрованих систем безпеки, ініціатором і засновником яких вона і має бути. Відтак, **геостра-тегічне розташування України передбачає наявність національних інтересів у різних частинах світу, що** потребує розроблення стратегій, програм і технологій їх адекватного забезпечення.

Наша позиція полягає у тому, що у ролі виразника і гаранта захисту національних інтересів має виступати держава. Національний ідеал, мета, ідея, потреби, цінності та інтереси - ті першоджерела, основні рушійні сили системи національної безпеки, що визначає її зміст, характер, архітектуру, спрямування. Проте слід констатувати, що в Україні, взагалі склалася парадоксальна ситуація, оскільки після прийняття Закону України «Про осно-

 ви національної безпеки України» тепер відсутня така категорія, як пріоритетні національні інтереси, натомість з'явився новотвір «пріоритети національних інтересів». Але навіть, не зважаючи на такі законодавчі хитросплетіння, досі відсутня методологія віднесення тих чи інших інтересів до пріоритетних, що утруднює формування системи національних інтересів, вичленення серед них життєво важливих, важливих та інших національних інтересів. Це у свою чергу, утруднює формування не лише національних інтересів в конкретних сферах життєдіяльності, а й взагалі підходів до розв'язання цього завдання.

Через це, подеколи трапляється груба фальсифікація національних інтересів, які підмінюються вузькопартійними, суб'єктивними, а подеколи й клановими інтересами окремих осіб, соціальних груп, олігархічно-територіальних кланів. Невизначеність цих питань створює поживний ґрунт для маніпулювання цією категорією. У більш загальному плані можна зазначити, що аморфність національних інтересів, позбавляє сенсу існування системи національної безпеки (СНБ), цілеспрямованість якої детермінована метою забезпечення пріоритетних національних інтересів, що безперечно становить серйозну загрозу національній безпеці.

Дослідження національних інтересів в інформаційній сфері із застосуванням методології націобезпекознавства має закласти ґрунт для формування системи національних інтересів у даній сфері із окресленням механізмів їх чергування, визначення пріоритетності.

Фундаментальний національний інтерес України - реалізу-ючи могутній потенціал великої європейської держави, посісти адекватне своїм бажанням і можливостям місце у світовому співтоваристві. Становлячи першооснову національної безпеки, ***національні інтереси*** можуть розглядатися в якості усвідомлених особово і суспільством, гарантованих державою цільових настанов щодо необхідності існування та розвитку людини, нації і держави як цілокупного організму.

Національні інтереси мають численні *стратегії їх забезпе чення.* У даному випадку ми одразу ж зауважимо, що під *стратегією* розуміємо програму організаційних дій, яка визначає ефективне функціонування і розвиток системи забезпечення національної безпеки, а також відповідну стратегію управління. У свою чергу, під *стратегією управління* і даному дослідженні ми розумітимемо основні напрями управлінської діяльності по досягненню стратегічної мети управління - забезпеченню реалізації національних інтересів.

Україна має твердо й чітко відстоювати власні національні інтереси, через що у керівному документі з питань державної політики національної безпеки - Концепції національної безпеки — мають бути закріплені фундаментальні положення щодо можливостей та умов застосування воєнної сили[37].

Перебуваючи в епіцентрі непримиренних ідеологій, розташована на роздоріжжі різних цивілізацій, Україна не має права, та у принципі й можливості, лишатись осторонь питань розбудови систем загальноєвропейської і глобальної безпеки, через що позаблоковий статус держави є атавізмом і потребує зміни. Україна має рішуче і твердо забезпечувати власну національну безпеку, застосовуючи увесь арсенал засобів, що є на озброєнні, передусім інформаційних. У найближчій перспективі необхідно розглядати можливість підсилення інформаційної складової національної безпеки України.

/. *Поняття «національних інтересів» і його відмінність від поняття «національна безпека»*

Поняття ***«національні інтереси»*** є ключовим при аналізі системи національної безпеки, а відтак і важливим для наукового аналізу в межах націобезпекознавства. Від їх визначення

[37] *Див.: Кондратьев Я.Ю., Ліпкан В А. Концепція національної безпе ки України: теоретико-правові аспекти зарубіжного досвіду. - К.: На ціональна академія внутрішніх справ України, 2003. - 20 с.*

В. А. ЛІПКАН, Ю. Є.МАКСИМЕНКО, В. М. ЖЕЛІХОВСЬКИИ залежать напрями функціонування СНБ, через що, дане поняття потребує детального розгляду. На цій обставині зосереджують увагу чимало дослідників, зазначаючи, що національні інтереси в методологічному сенсі являють собою першооснову інструментарію і механізму дослідження системи забезпечення національної безпеки як такої, оскільки створення та функціонування останньої зумовлено метою захисту національних інтересів країни[3]".

Аналіз геополітичних подій у світі уможливлює дійти висновку про безальтернативну необхідність існування в державі власної системи національної безпеки. Останнім часом геополітика стала втрачати свої позиції, значно поступаючись геоекономіці. Геоеко-номіка стала визначити геополітику, змінюючи геостратегії тих чи інших держав. Крім того, в умовах формування поліполярного світу відсутність ефективно діючої системи національної безпеки може призвести до втрати незалежності. За даних умов СНБ є суттєвим важелем і гарантом функціонування незалежної держави. Саме та держава, де ефективно діє СНБ, є уособленням інтересів особи і суспільства, саме така держава, забезпечуючи розвиток цих інтересів, сприяє зміцненню власних інститутів, а отже, спрямовує поступ нації до процвітання і прогресивного розвитку.

На сучасному етапі розвитку України державна політика національної безпеки має бути орієнтована, насамперед, на під-

[38] *Левицька М.Б. Теоретико-правові аспекти забезпечення національної безпеки органами внутрішніх справ України: Дис.... канд. юрид. наук; 12.00.01 / Нац. акад. внутр. справ України. - К., 2002. - С. 37. ; Валевский О.Л., Гончар ММ. Структура геополітичних інтересів України: Монографія. - К.: Нац. ін-т стратегічних досліджень, 1995. - 94 с; Ковальський В., Маначинський О., Пронкін Є. Національні інтереси: загрози та їх нейтралізація // Віче.- №7.- 1994. - С.57 - 62.; Косевцов В.О., Бінько І.Ф. Національна безпека України: проблеми та шляхи реалізації пріоритетних національних інтересів: Монографія. Сер. «Національна безпека>>. - Вип. 1. - К.: Національний ін-т стратегічних досліджень, 1996. - 53 с*

тримку соціально-політичної та інформаційної безпеки суспільства. Лише сформувавши монолітний соціум, об'єднавши його спільною ідеєю побудови незалежної держави, забезпечивши достатній рівень життя населення, можна говорити про національні інтереси та будувати їх ієрархію, від якої залежатимуть напрями функціонування СНБ.

Амбівалентність[39] таких категорій як особа, суспільство і держава, які виступають, з одного боку, як суб'єкти НБ, а з іншого, - як об'єкти, звичайно ж визначає і характер діяльності СНБ. Проте, віддаючи належне безпосередній участі конкретних громадян, громадських організацій і підсистеми недержавного забезпечення національної безпеки загалом, зауважимо, що провідну роль має відігравати держава.

Тому ефективним механізмом забезпечення цілісності особи, суспільства і держави як єдиного організму є *державне управління національною безпекою.* Незважаючи на пріоритет та цінність інтересів конкретної особи, будь-яка розвинена країна світу будує власну систему через примат державного управління. Це не означає фактичного виключення конкретних громадян і громадських організацій з процесу забезпечення національної безпеки. Навпаки, забезпечуючи диференціацію, держава створює в межах СНБ велику і вагому підсистему забезпечення - недержавну[0]. Аргу-

[39] *Одночасна наявність двох протилежностей.*

[40] *Назаров В.В. Деякі аспекти забезпечення безпеки підприємни цької діяльності // Недержавна система безпеки підприємництва як складова національної безпеки України.- К.: Вид-во Європ. ун-ту, 2004. - С. 230 - 237.; Крысин А.В. Безопасность предпринимательской деятельности. - М.: Финансы и статистика. 1996. - 384 с; Кузнецов СА. Роль негосударственных структур в обеспечении региональной безопасности Российской Федерации // Национальная безопасность и геополитика России. - 2001. - № 2 - 3. - С. 87 - 89.; Ліпкан ВА. Органі зація недержавної системи безпеки: Дипломна робота / Європейський університет фінансів, інформаційних систем, менеджменту та бізне су.- К., 2003.- 110с.*

В. А. ЛІПКАЯ, Ю. Є.МАКСИМЕНКО, В. М. ЖЕЛІХОВСЬКИИ ментом на користь нашої позиції є теза *ЮАДмітрієва,* що існують вагомі підстави ставити проблему виникнення загроз національній безпеці з боку самої держави". Підсистема недержавного забезпечення за даного випадку виступатиме гарантом, механізмом стримування і противаг. Втім функціонування останньої, яка становить собою хоча і суттєвий, але лише компонент, має бути узгодженою з генеральною лінією державної політики національної безпеки. З метою цієї синхронізації і організується система управління національною безпекою, складовими компонентами якої мають бути підсистеми державного і недержавного забезпечення'[2].

Поняття *«національні інтереси»,* які *«національна безпека»,* являє собою інтегративне утворення. Від його визначення залежить встановлення співвідношення інтересів особи, суспільства і держави, а в більш абстрактному плані - напрям прямування держави. Визначення національних інтересів має першочергове значення при створенні системи національної безпеки, через те, що саме заради ефективного їх забезпечення по суті і створюється дана система.

Одразу ж зупинимось на одному питанні, яке доцільно розглянути зараз: це питання *співвідношення* таких понять *як національна безпека і національні інтереси.* Підкреслимо, що **національні інтереси є категорією більш широкою, ніж національна безпека.** Крім того, національна безпека сама є як національний інтерес, адже забезпечення безпеки особи, суспільства та держави є неодмінною умовою виживання країни, без чого стає неможливими досягнення цілей іншого порядку. Отже існує реальна небезпека злиття предметів національних інтересів і власно на-

[41] *Дмитриев ЮА., Петров СМ., Идрисов Р.Ф. Государство как субъ ект обеспечения национальной безопасности России // Право и поли тика.- 2001.- № 11.-С. 64- 71.*

[42] *Ліпкан ВА. Теоретико-методологічні засади управління у сфері національної безпеки України: Монографія. - К.: Текст, 2005. - 350 с.*

ціональної безпеки". Це сприяє тому, що до проблематики національної безпеки відносять будь-які проблеми, тим самим суттєво розмиваючи саму цю проблематику. У даному аспекті, зазначимо, що національна безпека спрямована на створення умов для реалізації національних інтересів, у той час як реалізація останніх формує передумови для досягнення національного ідеалу та мети, а також реалізації національної ідеї.

Вперше модель співвідношення національної безпеки й національних інтересів була запропонована американцем У. Лип-пманом, де національна безпека розглядається як частина національних інтересів (американська школа). Серед апологетів даної теорії варто також виділити: Б.Броуді, С.Браун, М.Каплан, Г.Моргентау, М.Гальперін, Г.Кан, Г.Кіссенджер, С.Хоффман, Дж.Шлессінгер, Д.Кауффман та ін. Сама концепція «національних інтересів», на думку провідних теоретиків (Ч.Берд, С.Браун, М.Каплан, Р.Юхансон), властива саме західноєвропейській та американській політичній культурі^.

Ще однією особливістю американської школи слід назвати розробку двох принципових підходів, один з яких пов'язує національну безпеку з могутністю держави, що створює ресурс захисту безпеки, а інший становить на перше місце міжнародне співробітництво як створення умов забезпечення національної безпеки'[5].

[43] *Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство. / Санкт Петербургский университет МВД России. - СПб.: Фонд «Университет», 2000. - С. 61.*

[44] *Гончаренко О.М., Лисицин Є.М. Методологічні засади розробки нової редакції концепції національної безпеки України . Національний інститут стратегічних досліджень Серія «Національна безпека». ви пуск 4, 2001*

[45] *Кормич БА. Організаційно-правові засади політики інформації! ноїбезпеки України: Монографія.- Одеса: Юридична література, 2003. 472 с, С 12*

В. А. ЛІПКАН, Ю. Є.МАКСИМЕНКО, В. М. ЖЕЛІХОВСЬКИИ Так, *Кормич Б А.* акцентує, що на початку XX ст. міжнародне право вже склалося в чітку систему, яка значною мірою обмежувала дії держав, і, таким чином, було необхідно найти виправдання порушенню цих обмежень. Обґрунтування ж зневаги до норм міжнародного права необхідністю захисту національної безпеки виявилося цілком дієздатним. На жаль, така сама доля спіткала і застосування категорії національної безпеки у внутрішній сфері, яка, знову-таки, почала використовуватися в США як привід для обмеження громадянських свобод, прикладом чого став Communist Control Act або Закон про контроль за комуністами 1950 р., згідно з яким будь-яка організація, яка визнавалася комуністичною, відразу оголошувалася незаконною і втрачала будь-які права'".

Різноспрямованість як самих потреб нації, так і розмаїття засобів їх задоволення певним чином впливає і на право. У цьому аспекті постає проблема щодо розмежування права, яке забезпечує поступ нації відповідно до загально визнаних людських цінностей, і право, що відбиває егоїстичні інтереси нації, які є понад усе, а отже і методи їх забезпечення розглядаються лише крізь призму їх доцільності і аж ніяк не співвідносяться із загальнолюдськими цінностями та ідеалами. З іншого боку постає коректність такого порівняння: якщо ми вважаємо, що правом є лише те, що відповідає загально визнаним людським цінностям, то що ми тоді розумітимемо під нормативною системою, створеною як інструмент управління системою національної безпеки, який, маючи за мету забезпечення інтересів власної нації, припускається пригнічення інтересів інших націй"[7]?

Як вірно резюмує *Ліпкан В А.,* позиція сильної держави, якою, безперечно, буде Україна, не у тому, щоб «відповідати світовим

[46] *Кормич БЛ. Організаційно-правові засади політики інформацій ної безпеки України: Монографія.- Одеса: Юридична література, 2003. 472с.,С13*

[47] *Ліпкан ВА. Правове забезпечення управління системою націо нальної безпеки* II *Науковий вісник НАВСУ. - 2002. - № 3. - с 19-24;*

стандартам», а у тому, щоб, ураховуючи національні потреби та інтереси, на підставі застосування механізму імплементації бути повноправним членом світового співтовариства, входити до нього, зберігаючи як внутрішню, так і зовнішню самостійність.

Дана теоретична проблема має важливе значення при оцінці політичних рішень з погляду їх відповідності національним інтересам, оскільки інтереси безпеки є складовим компонентом національних інтересів, відтак політичні рішення, що приймаються і котрі шкодять інтересам безпеки, шкодять і національним інтересам. Приклад, скорочення Збройних сил України до 2010 року до 100 тис. осіб є прямою загрозою інтересам безпеки України, оскільки її армія перетвориться на «загін швидкого реагування» або «сили спеціальних операцій», котрий буде не здатен забезпечити безпеку держави у війні шостого покоління. У той час, як світові держави зосереджені на формуванні повітряно-космічних сил, сил проти супутникової оборони Україні нав'язують модель Збройних сил у вигляді військ швидкого реагування, оскільки на думку західних «фахівців» і їх глашатаїв в Україні, для України у найближчому майбутньому не існує широкомасштабної загрози. Разом з цим, політично дане рішення є обґрунтованим, оскільки вступ України до євроатлантичних структур передбачає, передусім, відповідність стандартам НАТО. Відтак політична доцільність і інтереси безпеки за даного випадку є протилежними, а отже теоретичне дослідження питання є вкрай важливим, оскільки дає можливість дійти висновку про цілеспрямований розвал українських Збройних сил, перетворення України на державу, здатну захистити себе лише в конфліктах малої інтенсивності, але не здатною здійснити захист у разі ведення проти неї війни шостого покоління, а відтак ефективно відстоювати національні інтереси в сфері міжнародної безпеки.

Відповідно до ст. 1 Закону України «Про основи національної безпеки України», *національні інтереси* - життєво важливі матеріальні, інтелектуальні і духовні цінності українського на-

 роду як носія суверенітету і єдиного джерела влади в Україні, визначальні потреби суспільства і держави, реалізація яких гарантує державний суверенітет України та її прогресивний розвиток.

Природним є існування в кожної незалежної держави власних національних інтересів, що зазвичай, створює потенціал до їх конкуренції, а іноді і до конфронтації. Цей факт є апріорним, тому зіткнення національних інтересів має сприйматися як процес утвердження держави в тій ролі, яку вона бажає і реально може зайняти. Крім того, відповідно до філософії екзистенціалізму, саме цей процес зіткнення і слугує самоідентифікації системи як такої, що реально відображає та захищає національні інтереси. Інша річ, коли утвердження національних інтересів відбувається внаслідок пригнічення національних інтересів інших суверенних країн, або взагалі здійснюється всупереч загальновизнаним нормам співіснування людства. Хоча геополітичний аналіз подій у світі уможливлює дійти висновку про ігнорування цього правила державами з розвиненими СНБ. Цей чинник також свідчить на користь необхідності формування *національно достатньої СНБ* - такої системи національної безпеки, яка б максимально забезпечувала національні інтереси.

Становлячи першооснову національної безпеки, *національні інтереси* можуть розглядатися як усвідомлені особою і суспіль-ством, гарантовані державою цільові настанови щодо необхідності існування та розвитку людини, нації і держави як єдиного організму. Зваясаючи на строкатість підходів до визначення даного поняття, вважається за доцільне виокремити два головні підходи.

Актуальною залишається проблема використання цих категорій для обґрунтування незаконних дій. Якщо згадати історію інституціоналізації цих категорій, то з самого початку їх використання не мало правового обґрунтування, оскільки в 1904 році Теодор Рузвельт приєднуючи зону Панамського каналу, обґрунтовував це інтересами національної безпеки.

Представники *першого підходу* взагалі вважають за недоцільне визначати саме поняття, зосередивши увагу на окресленні сутнісних ознак, які характеризують національні інтереси. На-риклад, *Ф. Зеліков* визначає національний інтерес як *«неопера-ційну мету»,* систему переваг, яка лежить в основі політики. При чому, ураховуючи неможливість перерахування усіх інтересів нації, як усвідомлених її потреб, більїп продуктивним, на думку даного дослідника, вважається побудова ієрархії національних інтересів, за допомогою яких можна було б окреслити фундаментальні, базові, ключові інтереси нації, порушення забезпечення яких загрожує СПБ. Після побудови ієрархії національних інтересів можна приступати до формування політичних цілей, які (і в цьому плані можна погодитись із *Ф. Заліковим)* не є тотожними політичним бажанням".

Представники *іншого напряму* вважають за доцільне точно визначити поняття національних інтересів. *Косевцов В.О. та Бінько І.Ф.*[49]*, Парахонський Б.О.*[Г'°]*,* а також інші науковці" визначають національні інтереси як конкретні історичні відносини і переконання, матеріальні, культурні та історичні цінності, що мають загальне життєво важливе значення для стабільного функціонування суспільства.

[48] *Почепцов Г.Г. Національна безпека країн перехідного періоду: Навч. посіб. - К., 1996. - С 10.*

[49] *Косевцов В.О., Бінько І.Ф. Національна безпека України: проблеми та шляхи реалізації пріоритетних національних інтересів: Моногра фія. Серія «Національна безпека». Випуск 1. - Київ: Нац. ін-т стратег, досліджень, 1996.- 53 с*

"" Парахонський Б.О. Національні інтереси України (духовно -інте-лектуальний аспект): Монографія. Сер. «Наукові доповіді».- Вип.6. -К-1993. -43 с

[51] *Соломатова В., Косолапова В., Гірник А. Національні інтереси У к раїни: структура суб'єктивних уявлень// Вісн. АН України.-1994.-31-С. 72- 76.*

З філософської точки зору національні інтереси є, в певній мірі, суб'єктивними уявленнями про фундаментальні цінності, які, в свою чергу, є відображенням потреб народу, що формуються в результаті діяльності'[2].

В. Тихии і М. Панов зазначають, що людина постійно дбає про захист своїх прав і свобод від тих чи інших посягань, небезпечних явищ, прагне до безпеки, бо це благо є вічною природною потребою, умовою для життєдіяльності людини. Саме держава в особі державно-правових інституцій покликана забезпечувати реалізацію усвідомлених потреб людини та загалом суспільства[53].

Цікавою для розгляду є думка *В. Ковальського, О.Мана-чинського, Є. Пронкіна,* які визначають **національні інтереси** як реальну причину дій нації й держави, цілеспрямованих на своє виживання, функціонування й розвиток, ... сукупність національних цілей і базових цінностей, які відіграють важливу роль у стратегії й тактиці в галузі національної безпеки[5'].

Характеризуючи дане визначення можна зазначити, що в ньому містяться окремі головні елементи, на базі яких формуються національні інтереси, зокрема національні цілі та цінності. Водночас із даного визначення важко зрозуміти, що є визначальним - національні інтереси для національних цінностей та цілей чи навпаки. Крім того, у понятті відсутнє посилання на такі важливі елементи, як національні потреби, національний ідеал, національну ідею тощо. Адже саме їх усвідомлення є рушійною причиною об'єктивації національних інтересів. У даному

[52] *Философский энциклопедический словарь / Редкол: С.С. Аверинцев. ЭА. Араб Оглы, Л.Ф. Ильичёв и др. - 2-е изд.- М.: Советская энцик лопедия, 1989. 815 с, С. 234*

[53] *Панов М., Тихий В. Безпека як фундаментальна категорія в ме тодологи правознавства (до постановки проблеми) // Вісник Академії правових наук України. - 2001. - № 3 (22). - С. 10 - 16.*

[5-1] *Ковальський В.,Маначинський О., Пронкін Є. Національні інтереси: загрози та їх нейтралізація // Віче.- № 7. - 1994. - С. 57.*

аспекті більш вдалим вважається визначення, запропоноване *О.В.Лупаїною:* національні інтереси - ціле, в якому відображені не будь-які, а найбільш спільні, схожі ознаки його устремлінь, бажань, цінностей відповідно до Божих Основ і законів Світобудови[5,5].

Національні інтереси відбивають стан суспільних відносин у внутрішній і зовнішній сферах, за якого можливе ефективне їх забезпечення. При чому, вони характеризуються динамічністю і відображають прагнення народу щодо власного розвитку в певний історичний період.

Використання методології НБЗ дозволяє нам розглядати національні інтереси як систему, якій притаманні загальні ознаки СНБ. Це, *по-перше,* відносна сталість національних інтересів, їх детермінованість і корелятивність ідеалам, цілям ідеї, потребам і цінностям української нації, а отже, ієрархічність; а *по-друге,* динамізм національних інтересів, їх обумовленість національними пріоритетами в певний історичний період. Саме тому національні інтереси, відбиваючи прагнення до розвитку української нації, становлячи ядро національної самосвідомості, характеризуються динамізмом.

Вивчення даного питання дозволяє розглядати його в кількох аспектах. *По перше,* національні інтереси можуть аналізуватися як у вузькому, так і широкому розумінні. У *вузькому* може йтися про інтереси титульної нації, в *широкому* - під національними інтересами розуміють систему істотних ознак і обставин існування української нації (особи, державних і недержавних інституцій) від її генезису до сьогодення. *По-друге,* відповідно до головних об'єктів національної безпеки, категорія «національний інтерес» співвідноситься з такими поняттям як «особистий інтерес», «державний інтерес». При цьому, слід акцентувати увагу не лише на рисах, що відрізняють ці групи інтересів, а й

[55] *Лупаина О.В. Основы национальной безопасности России в XXI веке II Национальная безопасность и геополитика России. - 2001. -М4-5.-С. 14.*

 на тих, що споріднюють їх, утворюючи власне категорію «національний інтерес».

Розглядаючи визначення поняття «національні інтереси», можна дійти висновку, що стосовно них, зазвичай, вживаються певні дії щодо забезпечення, напрями яких ми окреслили, аналізуючи стратегії забезпечення національних інтересів. Водночас категоричність окремих авторів щодо означення імовірних альтернатив дій щодо «національних інтересів» лише просуванням, захистом або пригнобленням (придушенням) не здається однозначно правильною[16]. Детальніше про це йтиметься під час розгляду питань забезпечення національної безпеки.

Численність підходів до визначення поняття національних інтересів зумовлена як складністю і багатоманітністю національних інтересів, так і несформованістю та невизначеністю їх змісту. На цьому шляху, на нашу думку, доцільним є дослідження змісту національних інтересів через окреслення їх виявів в об'єктивній дійсності, чому слугує їх ця класифікація".

Семантичний аналіз науково-практичних літературних джерел дає підстави дійти висновку про виокремлення трьох основних підходів до поняття «інтерес».

1. Інтерес як об'єктивна умова існування суб'єкта, предметом задоволення є щось матеріальне.

2. Інтерес як суб'єктивна спрямованість на певний результат (єдність об'єктивної та суб'єктивної сторони інтересу).

3. Інтерес як суспільні відносини, які є запорукою реалізації відповідних потреб.

[56] *Нижник Н.Р., Ситник Г.П., Білоус В.Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): Навч. посіб. для вищих навч. закл. / За заг. ред. П.В. Мельника, Н.Р. Нижник. - Ірпінь, 2000. - 304 с; Шевченко В., Костенко Г. Концепція національ ної безпеки: методологічний аспект // Голос України. - 1996. -11 січ.*

[57] *Ліпкан ВА. Теоретичні основи та елементи національної безпеки України: Монографія. - К.: Текст, 2003. - С 308 - 31 7.*

Останній підхід є найбільш поширений в правовій літературі.

Отже, враховуючи вищевикладене, під національним інтересом будемо_розуміти обумовлену національним ідеалом, національною метою та національною ідеєю систему загальнозначи-мих, усвідомлених та визнаних потреб і національних цінностей, яка забезпечує умови та засоби їх задоволення та реалізації.

2. Обумовленість національних інтересів

Після набрання чинності Закону України «Про основи національної безпеки України» були визначені пріоритети національних інтересів, а саме:

- гарантування конституційних прав і свобод людини та громадянина;
- розвиток громадянського суспільства, його демократичних інститутів;
- захист державного суверенітету, територіальної цілісності та недоторканності державних кордонів, недопущення втручання у внутрішні справи України;
- зміцнення політичної і соціальної стабільності в суспільстві;
- забезпечення розвитку і функціонування української мови як державної в усіх сферах суспільного життя на всій території України, гарантування вільного розвитку, використання і захисту російської, інших мов національних меншин України;
- створення конкурентоспроможної, соціально орієнтованої ринкової економіки та забезпечення постійного зростання рівня життя і добробуту населення;
- збереження та зміцнення науково-технологічного потенціалу, утвердження інноваційної моделі розвитку;
- забезпечення екологічно та техногенно безпечних умов життєдіяльності громадян і суспільства, збереження навколишнього природного середовища та раціональне використання природних ресурсів;

- розвиток духовності, моральних засад, інтелектуального потенціалу українського народу, зміцнення фізичного здоров'я нації, створення умов для розширеного відтворення населення;

- інтеграція України в європейський політичний, економічний, правовий простір та в євроатлантичний безпековий простір;

- розвиток рівноправних взаємовигідних відносин з іншими державами світу в інтересах України [5S].

Аналізуючи ряд досліджень, що присвячені розгляду проблематики національної безпеки, можна сказати, що практично всі роботи на чільне місце ставлять національні інтереси, залишаючи поза увагою національну ідею та національний ідеал.

Деякі дослідники говорять про те, що усвідомлені національні інтереси становлять основу внутрішньої та зовнішньої політики держави, визначають ідеологію державної системи[59].

Ми ж підтримуємо думку тих дослідників (Медведчук В.[60], Ліпкан В. Кириченко В.), які вважають, що національні інтереси мають похідний, вторинний характер щодо національної ідеї та, взагалі, доречно вести розмову про певну понятійну ієрархію: **національний ідеал — національна ідея — національні інтереси. І** ось чому.

Мала енциклопедія етнодержавознавства визначає **національний ідеал як сукупність уявлень того чи іншого народу про найдосконалішу модель свого національно-соціального устрою, яка найповніше відповідає його традиційним культурно-психо-**

[5S] *Про основа національної безпеки України: Закон України // Офіційний Вісник України. - 2003. -* V? *29. - Ст. 1433*

[59] *Левицька М.Б. Теоретико-правові аспекти забезпечення національної безпеки України органами внутрішніх справ України: Дис... канд...юрид. наук / 12.00.01 - К., 2002. - 206 с, С.76*

[e0] *Медведчук В.В. Сучасна українська національна ідея і актуальні питання державотворе)іня: Дис.... д-ра юрид. наук: 12.00.01.^ 12.00.02 / Нац. акад. внутр. справ України. - К., 1997.*

логічним установкам і забезпечує подальший розвиток: кінцеву мету національно-визвольного руху"'.

Етимологічно «ідеал» означає взірець досконалості, кінцева, найвища мета прагнень; ідеальний образ, що визначає спосіб мислення й діяльності людини"-.

Національна ідея **ж** формується на основі національного ідеалу, тобто є певним способом досягнення національного ідеалу.

Автори вищезазначеної енциклопедіїдіід **національною ідеєю розуміють реакцію самозбереження суспільності, середовища існування і розвитку індивідів, національної своєрідності народів, потреби у розбудові національного життя, стимулювання національно-відроджувального процесу"'.**

Медведчук В.В. зазначив, що будь-яка національна ідея, акумулює у собі найбільш значні, позитивні для суспільства інтереси, які склалися у суспільстві і сприймаються переважною більшістю населення, у першу чергу відповідним етносом, як необхідні для його подальшого розвитку, забезпечення добробуту народу".

Отже, національна ідея має вторинний характер від національного ідеалу. Вона не тільки базується та розвивається на його основі, але й забезпечує досягнення національного ідеалу. В свою чергу, національна ідея включає національні інтереси, які виступають теж є певним шляхом реалізації національної ідеї.

[61] *Мала енциклопедія етнодержавознавства / НАН України Ін-т де ржави і права ім. В.М. Корецького; редкол.: Ю.І. Римаренко (відп. ред.) та ін. - К.: Довіра; Генеза, 1996. - 942 с, С 108*

[62] *Словник іншомовних слів/ За ред. О.С. Мельничука. - К., 1974. - 775 с.*

[63] *Римаренко Ю. Етнополітичний організм // Мала енциклопе дія етнодержавознавства / НАН України Ін-т держави і права ім. В.М.Корецького; редкол.: Ю.І.Римаренко (відп. ред.) та ін.- К.: Довіра: Генеза, 1996.-495 с*

[64] *Медведчук В.В. Сучасна українська національна ідея і питання державотворення. - К.: Україна, 1997. - 170 с*

Таким чином, національний ідеал, національна ідея та національні інтереси є діалектично та ієрархічно взаємопов'язаними.

Особливо гострою є проблема збалансування інтересів представників усіх етносів, що компактно проживають на території України та представника титульної нації, оскільки Україна є поліетнічною державою.

З цього приводу є досить цікавою та слушною позиція Медвед-чука В.В., який зазначив, що коли ми будемо стверджувати, що в українському суспільстві панівне становище займає принцип «двоетнічності» (йдеться, власне, про український та російський етноси), або взагалі «поліетнізму » , який визнає існування на рівному соціальному статусі декількох етносів, то сама концепція ідеї втрачає свій сенс. З іншого боку, не можна погодитися й із застосуванням принципу «моноетнічності» України, оскільки у реальному житті він обов'язково проявить себе у гаслі «Україна для українців», що неминуче призведе до етнічного протистояння. Тому, і це знайшло своє закріплення в Конституції України 1996 року, загальновизнаною є модель так званого «титульного етносу», яким є український етнос, а також «етнічних меншин», до яких належать представники усіх інших етнічних груп, незважаючи на їх чисельність. Саме такий підхід відповідає міжнародній практиці етнодержавотворення, яка в питаннях прав людини і громадянина не визнає жодних привілеїв для представників титульної нації[6,5].

Ще однією проблемою є намагання певних політичних сил використання таких категорій як «національна ідея» та «національний інтерес» для реалізації власних інтересів.

Саме тому, формування національної ідеї має відбуватися природним шляхом, у ході розвитку суспільства, а активність з боку тих чи інших державних інституцій при цьому повинна зводитися до найбільш точного і повного вираження дійсного змісту

[65] *Медведчук В.В. Сучасна українська національна ідея і актуальні питання державотворення: Дис. ... dpa юрид. наук: 12.00.01., 12.00.02 / Нац. акад. внутр. справ України. ~ К., 1997., С. 42*

національного інтересу (системи інтересів) та сформульованої на цій основі національної ідеї"".

Кожному історичному періоду розвитку суспільства та держави відповідно властиві змістовні зміни в національних інтересах.

Це не означатиме зміну напряму пріоритетів цієї ідеї, а свідчитиме про постійний пошук життєздатних моделей розвитку української нації, її утвердження в якості сильної, прогресивної та гуманістичної нації через реалізацію національних інтересів. Причому національна ідея, становлячи собою продукт мислення української нації, дієво втілюватиметься у дійсність, а отже відображатиме рівень розвитку нації на тому чи іншому етапі еволюції. Можна навіть сказати, що національна ідея є відбиттям національного інтелекту, адекватного, з одного боку, реаліям існування української нації і її можливостям до втілення цієї ідеї, а з іншого — тим ідеалам, моделям існування, до яких вона постійне прагне[67].

Враховуючи вищевикладене, вважаємо доречною думку дослідників, які зазначили, що при формуванні національної ідеї слід мати на увазі такі аспекти:

1) національна ідея не повинна проголошувати титульний етнос виключним, через що надавати йому суттєві переваги перед іншими етносами, що складають ту чи іншу націю;

2) національна ідея має бути синтетичною, тобто включати як інтереси титульної нації, так і інтереси етнічних меншин, що проживають на території країни;

3) національна ідея має бути інтегративною, тобто об'єднувати інтереси титульної нації і етнічних меншин;

4) при побудові національної ідеї слід використовувати на ступний принцип: однаковість індивідів - загибель для популя-

[66] *Медведчук В.В. Сучасна українська національна ідея і актуальні питання державотворення: Дис. ... д-ра юрид. наук: 12.00.01., 12.00.02 / Нац. акад. внутр. справ України. - К., 1997., С. 37*

[67] *Ліпкан В А. Історичні передумови формування сучасної українсь кої національної ідеї // Вісник Національного університету внутріш ніх справ. - 2002.- № 19.- С 17 - 26., С. 18*

ції. Отже, національна ідея не має урівнювати усіх членів нації, стандартизувати їх відповідно до окреслених настанов. Навпаки, розмаїття етносів, об'єднаних спільною національною ідеєю, і є запорукою її тривалого, а головне — усвідомленого існування;

5) національна ідея має відбивати об'єктивні прагнення та інтереси нації на конкретно визначеному історичному етапі розвитку. Будь-які суб'єктивістські намагання забарвити національну ідею у власний колір, надаючи їй або релігійного, або політичного, або іншого змісту спаплюжать ідею, підміняють її на утилітарні прагнення, індивідуальний інтерес. Саме тому національна ідея не може ґрунтуватись на гаслі богообраності та на інших гаслах, які за своєю суттю створюють вакуум нації, роблячи її окремішною, месіанською і недосяжною для інших, створюючи об'єктивні передумови для її возвеличення;

6) національна ідея, будучи за своїм змістом гуманістичного напряму, має включати для своєї реалізації лише ті засоби, які передбачає національне та міжнародне законодавство. Будь-які засоби, застосування котрих веде до порушення законодавства (чи то тероризм, чи то геноцид, чи то диверсії, чи то війни тощо) суперечать самій суті національної ідеї, яка ґрунтується на засадах демократії та гуманізму;

7) ураховуючи поліетнічність України, наскрізною лінією має проходити толерантність титульного етносу до інтересів етнічних меншин[68].

*3. **Класифікація національних інтересів***

Слід зазначити, що саме питання про класифікацію *лише* національних інтересів не є безспірним. Так, наприклад, *В.В. Мед-ведчук* пропонує класифікацію запитів, потреб і інтересів:

[68] *Ліпкан В А. Історичні передумови формування сучасної української національної ідеї // Вісник Національного університету внутрішніх справ. - 2002. - № 19-С 17- 26.*

1) стосовно часу задоволення - запити, потреби, першочергові інтереси та інші;

2) стосовно суб'єкта, який має здійснити відповідні дії - людина, держава, громадські організації та різні самоврядні структури;

3) запити, потреби та інтереси, які притаманні усім членам суспільства - громадянам держави й ті, що цікавлять окремі його верстви;

4) запити, потреби й інтереси, що різняться за своїм характером - матеріальні та духовні"".

Звичайно, що категорія «національні інтереси» є багатокомпонентною. Через це постає необхідність у класифікації національних інтересів, виокремленні фундаментальних (базових), життєво важливих та інших груп національних інтересів. При цьому класифікація національних інтересів має розглядатися крізь призму необхідності виокремлення тих з них, завдання шкоди яким свідчить про національну небезпеку. Тобто кожному рівню національних інтересів кореспондуватиме певний рівень загрози СНБ. Знову таки, ураховуючи важливість даного положення, воно має бути відображено у Концепції національної безпеки України.

Отже, враховуючи різноманітні форми прояву, а також багатогранність самого феномену національних інтересів, їх багатоманітність і різноплановість, і відповідно до цього необхідність у впорядкуванні за певними критеріями, пропонується наступна їх класифікація.

За ступенем важливості

1. Життєво важливі національні інтереси - це такі національні інтереси, які пов'язані із виживанням і безпекою нації, захистом території України і території союзників, важливих

[63] *Медведчук В.В. Сучасна українська національна ідея і актуаль ні питання державотворення: Дис.доктора юрид. наук: 12.00.01., 12.00.02.1 Національна академія внутрішніх справ України. - К., 1997. - СІ 75.*

елементів інфраструктури, забезпеченням безпеки громадян та їх економічного добробуту. Життєво важливі інтереси можна визначати і як усвідомлені на рівні вищих органів державної влади *потреби* народу у збереженні й розвитку *національних цінностей,* національного багатства, вдосконалення економічного й політичного устрою суспільства. Для захисту інтересів цієї категорії Україна має рішучо використовувати усі наявні засоби, включаючи при необхідності, застосування своєї військової могутності.

Суттєвим для розуміння змісту життєво важливих національних інтересів є аналіз понять «національні потреби» і «національні цінності», тому окреслимо власне бачення щодо цього.

Під *національними потребами* слід розуміти такий стан нації, який обумовлений її незадоволеністю у нормальній життєдіяльності та спрямований на усунення цієї незадоволеності. Національні потреби реалізується у самому процесі їх задоволення. У разі ж незадоволення потреби нації це призводить до зміни нормальної життєдіяльності або ж до неможливості її подальшого існування. До реалізації потреби вона існує як такий недолік, що постійно з'являється і посилюється. З реалізацією потреби напруження, що виникло, послаблюється. Національні потреби є специфічними за своїм змістом, оскільки вони породжуються внаслідок генези самої нації — потреби у розвитку, у власній національній культурі, у власній державі тощо. Чим більшого розвитку досягає нація, тим більш широкий спектр потреб у неї виникає. Слід зважати на той факт, щоб при розвиткові потреб не виникало кардинальних розбіжностей у їх задоволенні серед представників різних національних меншин. Продуктивним вважається той шлях, за якого строкатість потреб буде поєднана із можливостями їх задоволення у загальних рамках національних інтересів. Для кожного представника української нації мають бути відкриті якнайширші можливості щодо засвоєння усіх створених предметів, здатних задовольнити духовні, інтелектуальні та матеріальні потреби, а отже до всебічного розвитку

потреб, передусім, у національному розвої, праці, творенні української нації, творчості на благо України. Всебічний розвиток національних потреб, створення предметів цих потреб і має бути національною необхідністю - потребою усіх.

Національні потреби тісно пов'язані із іншою, не менш важливою категорією — національні цінності. Під *національними цінностями* слід розуміти конкретно-історичні суспільні відносини й переконання, матеріальні та духовні об'єкти, що мають загально важливе значення для стабільного функціонування й розвитку народу. При чому національні цінності виступають як властивості явища, водночас вони не є притаманними йому від природи, і стають такими не через силу внутрішньої структури інтересів самих по собі, а через те, що вони є утягненими у сферу суспільного буття людини і стають носіями суспільних відносин. Щодо представників української нації, то національні цінності слугують об'єктами їх інтересів, а для їх свідомості виконують роль повсякденних *орієнтирів* у предметній і соціальній дійсності, визначень їх практичного ставлення до оточуючих предметів і явищ. Властивості тих чи інших явищ визначають різноманітні функції у системі людської життєдіяльності і виступають як предметні цінності, символи певних суспільних відносин, у яких бере участь людина. У якості національних цінностей можуть виступати деякі явища суспільної свідомості, які виражають ці інтереси в ідеальній формі (національний ідеал, національна мрія, національна справедливість тощо). До цього ж дані форми свідомості не просто описують якісь дійсні або уявні явища реальності, а виносять їм оцінку, схвалюють або засуджують їх, вимагають здійснення або усунення. Зіткнення різних за своїм змістом національних цінностей є наслідком боротьби різних стратегій, концепцій, доктрин, програм і технологій щодо забезпечення національної безпеки, які знаходять свій вияв у цілісних системах поглядів на сутність та зміст національного розвою, а у кінцевому рахунку - об'єктивну логіку історичного процесу. Саме

 тому визначення національних цінностей має ґрунтуватися не лише аксіологічно, а й з урахуванням свідомого розуміння об'єктивних історичних законів розвитку нації.

Отже, можна зазначити, що *українські національні цінності* — конкретно-історичні суспільні відносини й переконання, матеріальні та духовні об'єкти, визначені через усвідомлення об'єктивних історичних законів розвитку української нації, що мають конструктивне значення для стабільного функціонування й прогресивного розвитку народу України.

До *життєво важливих інтересів* безперечно належать: підтримка і збереження територіальної цілісності і недоторканності державного кордону України, забезпечення державного суверенітету; захист конституційного ладу усіма доступними засобами, включаючи військові, побудова ефективно діючої системи національної безпеки, утворення золотовалютного та алмазного фондів, всебічна інтеграція до створюваних систем глобальної безпеки, ініціативне створення систем безпеки різного рівня, інтеграція України у світове економічне і політичне співтовариство (входження до політичних та економічних структур Давосу, ВТО, ЄС тощо), розвиток національної економіки відповідно до національних інтересів, її унезалежнення від будь-якого зовнішнього втручання, створення умов для залучення іноземних інвестицій, забезпечення збереження старих та активізація пошуку нових шляхів доступу до стратегічно важливих для економіки ресурсів - нафти, енергоносіїв, всебічний розвиток відродження національної державності™.

Зі збереженням загального підходу, але із запропонуванням іншої назви щодо даної категорії національних інтересів, підходить *О.С.Бодрук,* який вживає поняття «корінні інтереси», до яких, на його думку, мають входити: збереження цілісності те-

[70] *Див. напр.: Ковальський В., Маначинсъкий О., Пронкін Є. Національні інтереси І/ Мала енциклопедіяетнодержавознавства /НАН України Ін-т держави і права їм. В.М.Корецького; редкол.: Ю.І .Римаренко (відп.ред.) та ін.. - К.: Довіра: Генеза, 1996. - С. 116.*

риторії держави; захист навколишнього середовища; конституційного устрою; політичної незалежності; забезпечення сприятливих умов розвитку нації; забезпечення зовнішньоекономічних пріоритетів держави; запобігання збройній агресії та силовій загрозі[71]. Водночас, поняття «життєво важливі національні інтереси» найбільш повно відображає сутність та зміст, а також значення даної категорії національних інтересів для прогресивного розвитку особи, суспільства і держави.

На основі цих інтересів має бути сформований *механізм національної безпеки* — сукупність цілей, функцій, принципів та методів, взаємодія яких забезпечує ефективне функціонування системи національної безпеки.

З урахуванням викладеного, до основних *цілей системи національної безпеки* по забезпеченню життєво важливих національних інтересів, можна віднести:

- максимально ефективне забезпечення національних інтересів;
- побудова розвиненої економіки;
- формування недержавної підсистеми забезпечення національної безпеки;
- формування дієздатних сил забезпечення національної безпеки;
- інформатизація суспільства;
- регіональне лідерство, одним з механізмів якого має стати ініціювання створення систем безпеки різних рівнів, де б Україна виступала лідером;
- побудова соціально-правової, демократичної держави, громадянського суспільства;
- формування позитивного іміджу України у світі;

[71] *Бодрук О.С. Структури воєнної безпеки: національний та міжнародний аспекти / Рада національної безпеки і оборони України; Національний ін-т проблем міжнародної безпеки. - К. : НІПМБ, 2001.-С.44-46.*

забезпечення збалансованого функціонування систем безпеки регіонального та вищих рівнів з урахуванням життєво важливих інтересів країн-учасниць.

Відповідно до окреслених основних цілей *функціями системи* мають бути:

- розумне співвідношення положень ринкової і адміністративної економіки, що відповідають національним особливостям української економіки;
- розроблення спеціального механізму гармонізації рекомендацій МВФ при проведенні економічних реформ (сумний досвід Аргентини довів, що сліпе виконання усіх вказівок, які відбуваються, передусім, на користь самого МВФ, а не держави, якій здійснюється допомога, призводить до колапсу економічної системи держави);
- розроблення системи заходів щодо забезпечення інформаційної безпеки України, як однієї з найважливіших складових національної безпеки;
- побудова сильної економічної системи, що сприятиме творенню України в міжнародних стосунках, її можливості брати участь у представницьких форумах найвищих рівнів, що позитивно впливатиме і на політичний імідж України, а це, у свою чергу, з урахуванням вигідного геостратегічного положення України, надасть їй можливість стати реальним лідером у регіоні;
- активізація процесів гармонізації законодавства й імплементації норм міжнародного права, які відповідають українським національним інтересам;
- максимально ефективно використання позитивного іміджу України для творення української стратегії;
- творення української стратегії та інші.

Основним *принципом, функціонування* даної системи має стати дуальна (подвійна) пріоритетність загальнолюдських цінностей і національних інтересів (принцип національної достатності). Зважаючи на цей факт, українські національні інтереси, як уособлення інтересів окремої особи і громадянина, що про-

живає на території України, мають враховуватись, насамперед, через те, що народ України є носієм суверенітету і єдиним джерелом державної влади.

Власно кажучи, життєво важливі інтереси відбивають фундаментальні, базові потреби нації, порушення або неможливість задовольнити які може призвести до її колапсу. Через це, природно, що кожна нація має власні, притаманні лише їй, національні інтереси. Цей суттєвий момент слід враховувати при створенні систем колективної, міжнародної, глобальної безпеки.

Життєво важливі інтереси є такими, що відбивають пріоритетні напрями розвитку нації, і їх порушення спричинює суттєвий дисбаланс СНБ. Отже, розроблення спільних життєво важливих інтересів держав-учасниць системи колективної безпеки є складним завданням, що ще раз свідчить про недоцільність розроблення категорії «всезагальний інтерес». Кожна нація має власні життєво важливі національні інтереси, які можуть бути лише враховані, але не пристосовані, або пригнічені через необхідність досягнення інтересів іншої нації, яка є членом утворюваної системи безпеки.

Так, дуже суперечливим є питання утворення різних коаліцій, які, передусім формуються за ініціативи тієї держави, яка хоче вирішити власні потреби, пояснюючи іншим про необхідність їх спільного рішення. При цьому наскрізною ідеєю створення деяких коаліцій є забезпечення інтересів держави-ініціатора, у той час, як деякі учасники цього утворення стають такими не в силу власних бажань чи потреб, а через прямий і латентний вплив. Утворення систем безпеки на таких засадах не сприятиме не лише забезпеченню життєво важливих інтересів нації, а навпаки - створить потенціал для майбутньої їх дестабілізації. Тому питання збалансованості життєво важливих інтересів кожної нації учасниці системи колективної безпеки, посідає чільне місце при розробленні систем різних рівнів. У цьому ж аспекті слід розглядати і створення уп равлінських структур, які відповідатимуть інтересам лише однієї нації-учасниці системи колективної безпеки.

Порушення або обмеження національних інтересів цієї групи свідчитиме про пряму загрозу системі національної безпеки, через що їх забезпечення має пріоритетне значення.

Система національних інтересів, являючи собою багатошаровий пласт, окрім життєво важливих інтересів уміщує також і інші категорії інтересів, необхідність у забезпеченні яких на тих чи інших етапах розвитку змінюється. Саме тому, поряд із вище розглядуваною категорією національних інтересів, слід говорити і про інші не менш важливі з них.

2. Важливі національні інтереси - такі національні інтереси, які не пов'язані із виживанням України, але які чинять вплив на добробут країни і характер міжнародної обстановки. Дана категорія національних інтересів на конкретному історичному етапі розвитку нації не відіграє ключової ролі, водночас завдання їм шкоди у перспективі закладає потенцію загрози життєво важливим інтересам. Порушення цих інтересів, хоча прямо і не загрожує СНБ, створює умови, за яких можуть бути обмежені життєво важливі інтереси. При чому віднесення тих чи інших інтересів до важливих характеризується часовим фактором. Відповідно до реалій об'єктивної дійсності, конкретного періоду, стану держави ті чи інші важливі інтереси можуть перейти до категорії життєво важливих. Так, наприклад, до подій на Чорнобильській атомній станції, національні інтереси в сфері екологічної безпеки належали до важливих, через їх, нібито, не життєву значущість і важливість. Нормальне функціонування АЕС, жорстка система контролю за ними давали можливість того часу саме таким чином ставитися до цієї групи національних інтересів. Але після аварії на ЧАЕС трапилися кардинальні зміни, і Україна, усвідомивши небезпеку екологічної катастрофи, переглянула власне ставлення, і відтоді національні інтереси в сфері екологічної безпеки набули статусу життєво важливих. Такі інтереси мають захищатися із використанням наявних ресурсів для досягнення своїх цілей, з урахуванням *домірності ціни та ризику із ступенем важливості* інтересів, що зачіпаються.

3. **Інші національні інтереси** - такі національні інтереси, яким можуть загрожувати стихійні лиха, великі виробничі катастрофи, порушення прав людини. Дана категорія інтересів відстоюватиметься через прийняття певних дій для усунення таких явищ і для захисту цінностей, які розділяє Україна: підтримання процесу демократизації, здійснення цивільного контролю над системою забезпечення національної безпеки, надання допомоги у розмінуванні, стимулювання послідовного розвитку.

За рівнем прояву

Наступним критерієм класифікації є *рівень прояву.* Відповідно можна виділити такі групи.

Внутрішні — дана група національних інтересів є домінантною. Передусім, цілісність українського соціуму, ефективно діюча економічна система держави, сучасна система національної безпеки, дієздатні сили забезпечення національної безпеки надають можливість претендувати Україні не лише на висунення і декларацію, а й на реальне забезпечення внутрішніх національних інтересів. Це означає, що лише міцна в економічному й оборонному відношенні Україна може стратегічно більш ефективно забезпечувати безпеку держави, суспільства і особи. Порушення цих складових може призвести до втрати суверенітету та незалежності держави[72].

Зовнішні національні інтереси базуються на внутрішніх і спрямовані на максимально ефективне забезпечення національних інтересів поза межами України. Національні інтереси України, яка є геополітичним центром Європи, не обмежуються її кордонами. Отже наявність зовнішніх національних інтересів має корелювати із можливістю їх забезпечення. А ця можливість, передусім, базується на стані забезпеченості внутрішніх національних інтересів. Саме тому можна казати про дуальність прояву національних інтересів, тобто про діалектичний зв'язок внутрішніх і зовнішніх інтересів, де забезпечення перших є виз-

[72] *Ковальський В., Маначинський О., Пронкін Є. Національні інтереси: загрози та їх нейтралізація // Віче.- №7.- 1994. - С. 62.*

начальним. Чим надійніше забезпечені внутрішні національні інтереси, тим більше можливостей має держава для забезпечення зовнішніх інтересів.

За ступенем стійкості

Стратегічні національні інтереси - це такі національні інтереси, забезпечення яких сприяє досягненню національного ідеалу. Остання категорія доволі цікава, через її фундаментальну важливість, тому окреслимо власне бачення щодо розуміння національного ідеалу.

Національний ідеал можна розглядати як нерозривну єдність *суспільного, морального* і *естетичного* ідеалів.

Суспільний ідеал української нації становить собою найбільш загальні уявлення тієї чи іншої соціальної групи, які відповідають її економічним і соціальним інтересам та є кінцевою метою її прагнень і діяльності. Суспільний ідеал має бути прогресивним, тобто відповідати об'єктивним тенденціям і бути ідейною основою розвитку суспільства.

Моральний ідеал становить собою уявлення про моральну досконаліть, яка знаходить свій вираз в образі особистості, яка втілила такі моральні якості й може слугувати моральним взірцем. Він відображає соціально-економічний і духовний розвиток суспільства і відповідає його критерію моральності та суспільному ідеалу. Моральний ідеал української нації передбачає патріотизм, толерантність, взаємодопомогу, гуманізм, усвідомлення пріоритету загальнолюдських цінностей, плекання національних традицій тощо. Найбільш повне наближення до морального ідеалу - мета морального виховання української нації.

Естетичний ідеал - історично найбільш повна і гармонійна єдність суб'єкта і об'єкта, окремого представника української нації в цілому і природи, яке знаходить вираз у вільному і універсальному розвиткові людських творчих сил як самоціль. Естетичний ідеал слугує критерієм оцінки прекрасного у житті та мистецтві. Естетичним ідеалом української нації можна вважати всебічний, цілісний і гармонійний розвиток творчих сил

кожної людини, яке уміщує в себе духовне багатство, моральну чистоту і фізичну досконалість української нації.

Отже, *національний ідеал* української нації можна визначити як ідейну основу, найбільш загальні уявлення української нації відповідно до об'єктивних тенденцій реальної дійсності про її соціально-економічний і духовний розвиток, гармонійна єдність суб'єкта і об'єкта, окремого представника і української нації в цілому та природи, які знаходить вираз у вільному і універсальному розвиткові нації і становлять собою кінцеву мету її прагнень і діяльності.

Національний ідеал не слід ототожнювати із національними інтересами, хоча останні є засобом досягнення першого. Головним критерієм вірності обраного національного ідеалу є його відповідність об'єктивним реаліям сучасної дійсності. І хоча при конструюванні національного ідеалу не можна відкидати історичне минуле, головним орієнтиром має бути сьогодення і майбуття. Інакше кажучи, ***кінцева мета нації*** - досягнення національного ідеалу, і на цьому шляху вона має вирішувати конкретні завдання, якими є національні інтереси.

Зазначимо, що зміст національного ідеалу визначається не лише економічними і соціальними, а й релігійними інтересами, моральними нормами, ідеями гуманізму, патріотизму та іншими ідеологічними побудовами. У даному контексті можна резюмувати, що **безальтернативний національний ідеал** України - це соборність, рівність і незалежність.

Розгляд змісту національного ідеалу дозволяє більш повно усвідомити необхідність у формуванні стратегічних національних інтересів. Ураховуючи викладене, зауважу, що загроза стратегічним інтересам означає загрозу життєво важливим інтересам нації. Дані інтереси мають бути визначені та закріплені відповідним чином у стратегіях, доктринах, концепціях, програмах. Причому стратегічні інтереси визначають життєво важливі інтереси. Опосередкування останніх першими відбувається через те, що пріоритетність тих чи інших національних інтересів, віднесення їх до

категорії життєво важливих має динамічний характер і обумовлене передусім тим, які конкретно завдання стоять перед українською нацією на певно визначеному історичному етапі розвитку.

Стратегічні національні інтереси закладають фундамент до стратегії управління системою національної безпеки, визначають головні цілі та напрями управлінської діяльності. Стратегічні національні інтереси посідають найвищий щабель ієрархії системи національних інтересів.

Тактичні національні інтереси - це конкретизовані стратегічні національні інтереси, які потребують впровадження у короткотерміновий період, вони є засобом впровадження стратегічних національних інтересів у життя. їх реалізація здійснюється для досягнення безпосередньої мети, вирішення найближчих завдань. На відміну від стратегічних національних інтересів, тактичні національні інтереси значно конкретніше, у той же час більш гнучкі, допускають варіативність у межах стратегічних національних інтересів. Тактичні національні інтереси формують механізм черговості національних інтересів, їх *ранжування* за ступенем важливості (тобто визначення, який з національних інтересів є пріоритетним) і *черговості* (бажаній послідовності їх реалізації з урахуванням реальних можливостей і характеру їх взаємозв'язку). Даний процес має грунтуватися на таких постулатах, як: єдина цілісна українська нація і самостійна, незалежна, соборна держава. Отже реалізація тактичних національних інтересів відбувається в межах стратегічних національних інтересів і спрямована на забезпечення останніх. У найбільш загальному плані тактичні національні інтереси співвідносяться із важливими національними інтересами.

Оперативні національні інтереси - це така сукупність національних інтересів, реалізація у життя яких дозволяє негайно впливати на конкретні відхилення від досягнення тактичних і стратегічних національних інтересів. У найбільш загальному плані вони співвідносяться із такою категорією, як інші національні інтереси.

Одним з чинників існування національних інтересів є просторовий, відповідно до якого національні інтереси не слід ототожнювати лише з тією територією, де розташована країна. Категорія «національні інтереси» має динамічний характер ще й тому, що саме націобезпекознавство, в контексті якого ми і розглядаємо поняття «національних інтересів», становить собою систему знань про забезпечення динамічної стабільності системи національної безпеки. Через це виникає необхідність у введенні щодо системи категорійно-понятійного апарату нашої теорії спеціального терміну, який би характеризував динамічність національних інтересів, їх просторову визначеність - *«сфера національних інтересів».*

За ступенем пріоритетності

За *ступенем пріоритетності* можна виділити:

пріоритетні національні інтереси - такі національні інтереси, які мають пріоритет на тому чи іншому етапі історичного розвитку країни, обумовлені об'єктивними потребами соціуму і його прогресивному розвитку і вимагають першочергових заходів щодо їх реалізації;

потенційно пріоритетні національні інтереси - такі національні інтереси, які за певних умов можуть стати пріоритетними. При чому виокремлення тих чи інших інтересів до даної категорії обумовлено результатами моніторингових досліджень, за допомогою яких виявляють динаміку розвитку процесів у сфері національної, і з огляду на це формують модельний ряд пріоритетних національних інтересів. Таким чином, національні інтереси, які не є пріоритетними, але перебувають в модельному ряді пріоритетних, і є потенційно пріоритетними національними інтересами;

звичайні національні інтереси - інші національні інтереси, які не входять до пріоритетних та потенційно пріоритетних національних інтересів.

Отже, з урахуванням наведеного, на сучасному етапі розвитку України у найбільш загальному плані можна виділити наступні національні інтереси:

- внутрішня стабільність, яка характеризується стійкістю державних інститутів і збалансованістю інтересів усіх соціальних груп населення;

- захист державного суверенітету, територіальної цілісності та недоторканності державних кордонів, недопущення втручання у внутрішні справи України;

- становлення України як правової держави, що захищає усіма законними важелями національні інтереси у будь-якій точці Земної кулі;

- економічне процвітання, задоволення матеріальних потреб населення, здатність до ефективного господарського розвитку: лише сильна в економічному плані держава може бути здатна до забезпечення власної національної безпеки, а також відігравати роль регіонального лідера;

- забезпечення розвитку і функціонування української мови як державної в усіх сферах суспільного життя по всій території України, гарантування вільного розвитку, використання і захисту інших мов національних меншин України;

- ефективне функціонування СНБ;

- побудова професійної армії, але, враховуючи сумний досвід колапсу Римської імперії, в армії мають служити виключно громадяни України;

- пріоритетність загальнолюдських демократичних принципів у розбудові держави, національна злагода та національна свідомість народу;

- гарантування конституційних прав і свобод людини і громадянина;

- підтримання екологічно здорового середовища;

- розвиток духовності, моральних засад, інтелектуального потенціалу Українського народу, зміцнення фізичного здоров'я нації, створення умов для розширеного відтворення населення;

- інтеграція України в європейський політичний, економічний, правовий простір та в євроатлантичний безпековий простір;

- розвиток рівноправних взаємовигідних відносин з іншими державами світу в інтересах України;

- формування національної стратегії, яка включатиме національний ідеал, національну мету, національну ідею, національні, потреби, національні цінності, національні інтереси, врешті-решт національну ідеологію;
- утвердження в якості регіонального лідера;
- формування позитивного міжнародного, передусім гуманітарного іміджу[73].

4. Національні інтереси в інформаційній сфері

Як зазначалось раніше, Закон України «Про основи національної безпеки України» не містить переліку національних інтересів в інформаційній сфері, а визначає виключно пріоритети національних інтересів, які є загальними для всіх сфер життєдіяльності людини, суспільства та функціонування держави, а також перелік загроз національним інтересам в інформаційній сфері та основні напрями державної політики з питань національної безпеки в інформаційній сфері. Спробуємо на основі вищезазначеного, а також положень Конституції, використовуючи ме^тод кореляції та догматико-юридичний метод, виокремити національні інтереси в інформаційній сфері.

Одразу зазначимо, що під ***національними інтересами в інформаційній*** *сфері* ми розуміємо визначальні потреби людини (громадянина), суспільства і держави в інформаційній сфері, реалізація яких гарантує інформаційний суверенітет України, а також прав та свобод людини в інформаційній сфері.

Таким чином, можна виокремити тріаду національних інтересів:

[73] *Див.: Ковальський В., Маначинський О., Пронкін Є. Національні інтереси: загрози та їх нейтралізація // Віче.- № 7. - 1994. - С. 58.; Валевський О.Л., Гончар М.М. Структура геополітичних інтересів України. - К.: НІСД, 1995. - С. 75.; Закон України «Про основи націо нальної безпеки України» // Офіційний Вісник України. - 2003. ~ № 29.- Ст. 1433.*

- людини та громадянина;
- суспільства;
- держави.

Саме ця триєдність є системоутворюючими елементами системи національних інтересів України, перебуваючи в тісному діалектичному взаємозв'язку та взаємодії. Тобто національні інтереси України - це інтегрований вираз консолідованих інтересів і людини, і суспільства, і держави.

Поділ національних інтересів в залежності від об'єкта (людини, суспільства, держави) є умовним з розумінням того, що негативна роль загроз розповсюджується одночасно на декілька чи значну кількість національних інтересів.

Зазначимо також, що об'єктом нашого наукового інтересу виступатимуть тільки національні інтереси людини, суспільства та держави в інформаційній сфері в контексті інформаційної безпеки, оскільки не всі інтереси в інформаційній сфері є об'єктом забезпечення інформаційної безпеки.

Аналіз Конституції України дозволив говорити про закріплення основних прав та свобод людини в інформаційній сфері.

Так, згідно зі ст. 15 суспільне життя в Україні ґрунтується на засадах політичної, економічної та ідеологічної багатоманітності. Жодна ідеологія не може визнаватися державою як обов'язкова. Цензура заборонена.

Ст. 31 зазначає, що кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції.

Ст. 32 Основного закону визначає, що не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею.

Ст. 34, в свою чергу, гарантує право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір.

Відповідно до ст. 41 кожен має право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності.

Близькою до цієї статті за змістом є ст. 54, згідно з якою громадянам гарантується свобода літературної, художньої, наукової і технічної творчості, захист інтелектуальної власності, їхніх авторських прав, моральних і матеріальних інтересів, що виникають у зв'язку з різними видами інтелектуальної діяльності. Кожний громадянин має право на результати своєї інтелектуальної, творчої діяльності; ніхто не може використовувати або поширювати їх без його згоди, за винятками, встановленими законом.

Даний комплекс прав та свобод вважається непорушним та невідчужуваним. В основу положень розділу II «Права, свободи та обов'язки людини і громадянина» Конституції України покладено ряд міжнародних нормативно-правових актів. Зокрема, Загальна декларація прав людини, Міжнародний пакт про економічні, соціальні і культурні права, Міжнародний пакт про громадянські та політичні права.

Загалом, на основі здійсненого аналізу вищевикладених норм Конституції України, а також беручи до уваги національні інтереси, визначені Законом України «Про основи національної безпеки України», можна виокремити, *основні національні інтереси в інформаційній сфері,* а саме:

а) для людини:

- реалізація прав і свобод людини і громадянина щодо одержання, використання, поширення, зберігання інформації;
- забезпечення права людини на захист від маніпуляції індивідуальною свідомістю;
- захист права інтелектуальної власності;

- захист енергоінформаційної безпеки людини тощо.

б) для суспільства:

- побудова інформаційного суспільства;
- забезпечення плюралізму засобів масової інформації;
- захист від маніпуляції масовою свідомістю;
- розвиток духовності, моральних засад, інтелектуального потенціалу Українського народу, зміцнення психічного здоров'я нації.

в) для держави:

- забезпечення інформаційного суверенітету;
- унеможливлення монополізації інформаційного простору іноземними компаніями або транснаціональними корпораціями;
- створення конкурентоспроможних інформаційних техноло гій та технологій зв'язку;
- збереження та зміцнення науково-технологічного потенціалу;
- інтеграція України в європейський інформаційний простір;
- боротьба з інформаційною злочинністю тощо.

Оскільки національні інтереси мають досить динамічний та строкатий характер, що унеможливлює закріплення навіть базових національних інтересів в інформаційній сфері, досить важливим є російський досвід розгляду цієї проблеми.

Так, в Доктрині інформаційної безпеки РФ закріплюється не перелік національних інтересів людини, суспільства та держави в інформаційній сфері, а здійснюється виокремлення чотирьох основних складових національних інтересів Російської Федерації в інформаційній сфері.

Перша складова національних інтересів РФ в інформаційній сфері полягає у дотриманні конституційних прав і свобод людини та громадянина в галузі одержання інформації й користування нею, забезпеченні духовного відновлення Росії, збереження й зміцнення моральних цінностей суспільства, традицій патріотизму, гуманізму, культурного й наукового потенціалу.

Друга - в інформаційному забезпеченні державної політики РФ, доведенні до російських громадян та міжнародної громадськості достовірної інформації про державну політику РФ, її офіційної позиції щодо соціально значимих подій у житті держави та міжнародного життя, із забезпеченням доступу громадян до відкритих державних інформаційних ресурсів.

Третя - у розвитку сучасних інформаційних технологій, вітчизняної індустрії інформації, у тому числі 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.

Четверта - у захисті інформаційних ресурсів від технічних розвідок, несанкціонованого доступу, забезпеченні безпеки інформаційних і телекомунікаційних систем.

Далі російським законодавцем затверджується ряд дій, які забезпечать реалізацію кожної групи національних інтересів в інформаційній сфері.

Висновки

Таким чином, з урахуванням проведених нами досліджень, пропонується категорія «національні інтереси в інформаційній сфері» доцільно розглядати крізь призму наступного категоріального ряду:

національний ідеал - національна мета - національна ідея - національні інформаційні потреби - національні інформаційні цінності - національні інтереси в інформаційній сфері - національна ідеологія[74].

Відповідно до викладеного, це ***національні інтереси в інформаційній сфері*** - це результат усвідомлення цінності інформа-

[74] *ЛіпканВА. Теоретичні основи та елементи національної безпеки України: Монографія. - К.: Текст, 2003.*

ційних потреб, свідомісний вибір національних інформаційних цінностей, які зумовлені національним ідеалом, метою та ідеєю і забезпечують умови та засоби їх задоволення і реалізації.

Під час своєї реалізації національні інтереси в інформаційній сфері стикаються з різними перешкодами, що іноді або створюють загрозу для їх реалізації, або спричинюють їх нереалізацію. У свою чергу, нереалізація національних інтересів в інформаційній сфері свідчить про недостатню ефективність функціонування системи національної безпеки в інформаційній сфері. Відтак основним питанням виживання України є створення адекватної сучасному стану України, її національним інтересам і загрозам системи інформаційної безпеки, яка б включала **сили та засоби ведення виграшних інформаційних війн.**

До основних ***національних інтересів в інформаційній сфері*** можна віднести:

1) інформаційна стабільність, яка характеризується інформаційною стійкістю державних інститутів як до внутрішніх, так і до зовнішніх інформаційних впливів;

2) інформаційна збалансованість, яка є адекватною мірою інтегрованості інформаційних інтересів усіх соціальних груп населення;

3) інформаційний суверенітет, недопущення втручання засобами інформаційного протиборства у внутрішні справи України;

4) становлення України як інформаційної держави, повноправного суб'єкта інформаційного суспільства та інформаційної цивілізації, яка створює уг.іма можливим інформаційними засобами умови для реалізації національних інтересів в інформаційній сфері у будь-якій точці Земної кулі;

5) інформаційне процвітання, задоволення інформаційних потреб населення, здатність до ефективного інформаційного роз витку: лише сильна в інформаційному плані держава може бути здатна до забезпечення власної національної безпеки, а також відігравати роль регіонального лідера і не залишитися на узбіччі інформаційної цивілізації;

6) забезпечення розвитку і функціонування української мови як державної в усіх сферах суспільного життя на всій території України, гарантування вільного розвитку, використання і захисту інших мов національних меншин України;

7) ефективне функціонування системи національної безпеки в інформаційній сфері;

8) побудова якісно нової армії, акценти в якій мають бути зроблені на оснащення найсучаснішою зброю і технологіями, у тому числі ведення інформаційних протиборств різних рівнів;

9) збереження культурних традицій українського народу, його укладу життя, історичної спадщини;

10) пріоритетність загальнолюдських демократичних при нципів у розбудові держави, національна злагода та національна свідомість народу;

11) гарантування конституційних прав і свобод людини і громадянина в сфері інформації;

12) підтримання інформаційно здорового середовища;

13) розвиток духовності, моральних засад, інтелектуального потенціалу Українського народу, зміцнення фізичного здоров'я нації, створення умов для розширеного відтворення населення;

14) інтеграція України в загальносвітовий інформаційний простір.;

15) розвиток рівноправних взаємовигідних відносин з іншими державами світу в інтересах України;

16) формування на базі стратегії стійкого розвитку і концепції національної безпеки доктрини інформаційної безпеки, яка включатиме національний ідеал, національну мету, національну ідею, національні інформаційні потреби, національні інформаційні цінності, національні інформаційні інтереси, врешті-решт національну ідеологію;

17) утвердження в якості регіонального лідера;

18) формування позитивного міжнародного, передусім гу манітарного іміджу.

національні інтереси, національні інтереси в інформаційній *сфері,* ***національний ідеал, національна ідея.***

Контрольні запитання для самоперевірки

1. Розкрийте зв'язок між категоріями «національна безпека» та «національні інтереси»?

2. У чому особливості американського погляду на співвідношення понять «національна безпека» та «національні інтереси»?

3. Які існують основні підходи до розгляду поняття «інтерес»?

4. Як співвідноситься між собою поняття «національні інтереси» та «пріоритети національних інтересів?

5. Які пріоритети національних інтересів закріплені законодавчо?

6. Розкрийте взаємозв'язок між поняттями «національний ідеал», «національна ідея» та «національний інтерес»?

7. Які основні моменти повинна охоплювати «національна ідея»?

8. Назвіть базові характеристики «національного інтересу»?

9. Які національні інтереси в інформаційній сфері Ви можете назвати?

Завдання для самопідготовки

1. З'ясуйте різницю між національним інтересом та цінністю в інформаційній сфері.

2. Який існує взаємозв'язок між національним інтересом та національною безпекою?

Список рекомендованої літератури

Нормативні джерела

1. Закон України про друковані засоби масової інформації (пресу) в Україні // Відом. Верховної Ради України. - 1993. -№ 1 -Ст. 1.
2. Закон України про захист інформації в автоматизованих системах // Відом. Верховної Ради України. - 1994. - № 31 -Ст. 286.
3. Закон України про інформацію // Відом. Верховної Ради України. - 1992.-№ 48. - Ст. 650.
4. Закон України про науково-технічну інформацію // Відом. Верховної Ради України. - 1993. - № 33 - Ст. 345.
5. Закон України про Національну програму інформатизації // Відом. Верховної Ради України. - 1998. - № 27-28. - Ст. 181.

Доктринальні джерела

1. *Гончаренко О.М., Лисицын Є.М.* Методологічні засади розробки нової редакції концепції національної безпеки Украї ни: Монографія. Серія «Національнабезпека». Випуск 4. - Київ: Нац. ін-т стратег, досліджень, 2001.- 56 **с**
2. Информационное пространство // Hi-Tech (Панорама высоких технологий). - 2002. - № 9. - С.6.
3. *Кормич Б А.* Організаційно-правові засади політики інформаційної безпеки України: Монографія.- Одеса: Юридична література, 2003.- 472 с
4. *Косевцов В.О., Бінько І.Ф.* Національна безпека України: проблеми та шляхи реалізації пріоритетних національних інтересів: Монографія. Серія «Національна безпека». Випуск 1. - Київ: Нац. ін-т стратег, досліджень, 1996.- 53 **с**
5. *Левицъка М.Б.* Теоретико-правові аспекти забезпечення національної безпеки України органами внутрішніх справ України: Дис...канд...юрид. наук / 12.00.01 - К., 2002. - 206 с

6. *Ліпкан ВЛ,* Історичні передумови формування сучасної української національної ідеї // Вісник Національного університе ту внутрішніх справ. - 2002. - № 19.- С. 17 - 26.

7. *Ліпкан ВЛ.* Правове забезпечення управління системою національної безпеки // Науковий вісник НАВСУ. -2002. - № 3.-с. 19-24.

8. Мала енциклопедія етнодержавознавства / НАН України Ін-т держави і права ім. В.М. Корецького; редкол.: Ю.І. Римаренко (відп. ред.) та ін. - К.: Довіра; Генеза, 1996. - 942 с.

9. *Медведчук В.В.* Сучасна українська національна ідея і актуальні питання державотворення: Дис. ... д-ра юрид. наук: 12.00.01., 12.00.02 / Нац. акад. внутр. справ України. - К., 1997.

10. *Панов М., Тихий В.* Безпека як фундаментальна категорія в методології правознавства (до постановки проблеми) // Вісник Академії правових наук України. - 2001. - № 3 (22). - С. 10 - 16.

11. *Парахонський Б.О.* Національні інтереси України (ду ховно -інтелектуальний аспект): Монографія. Сер. «Наукові до повіді».-Вип.6. -К.- 1993.-43 с

12. Словник іншомовних слів/ За ред. О.С. Мельничука. - К., 1974.- 775 с

13. *Соломатова В., Косолапова В., Гірник А.* Національні інтереси України: структура суб'єктивних уявлень// Вісн. АН України.-1994.-31.- С 72 - 76.

14. Философский энциклопедический словарь / Редкол: С.С. Аверинцев. Э.А. Араб-Оглы, Л.Ф. Ильичёв и др. - 2-е изд.- М.: Советская энциклопедия, 1989.- 815 с.

РОЗДІЛ 3 ПОНЯТТЯ ТА ЗМІСТ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Вступ

Відповідно до націобезпекознавчого підходу, загрози інформаційній безпеці, з одного боку являють собою організаційний компонент системи державного управління, а з іншого - слугують індикатором ефективності її функціонування. Адже реалізація загроз і переростання їх у небезпеки свідчить про неефективність функціонування даної системи, і навпаки. На сьогодні розглядати будь-які загрози в інформаційній сфері необхідно з урахуванням того контексту, в якому вони виникають і знаходять свій вияв. Найбільш небезпечною на даному етапі розвитку українського суспільства є проведення *інформаційних війн* -крайньої форми інформаційного протиборства.

Питання формування понятійного апарату у сфері інформаційних відносин ще остаточно не вирішені. І передусім це пов'язано із недостатнім застосуванням методології націобезпе-кознавства - теорії національної безпеки та її понятійного апарату[75].

У даному розділі ми розглянемо поняття «інформаційна боротьба», його співвідношення з іншими спорідненими поняттями, такими як «інформаційна війна», «інформаційне протиборство». Застосування структурного аналізу дозволить виокремити атрибутивні ознаки та встановити кореляційні зв'язки між існуючими поняттями суспільних явищ, що відбуваються в інформаційній сфері.

[75] *Ліпкан ВЛ. Теоретичні основи та елементи національної безпеки України: Монографія. - К.: Текст, 2003. - 600 с ; Ліпкан ВЛ. Тео-ретико-методологічні засади управління у сфері національної безпеки України: Монографія. - К.: Текст, 2005. - 350 с*

Поняття інформаційних війн

Передусім можна наголосити на тій обставині, що чисельність трактувань даного поняття, має більш глибинні коріння, ніж це здасться на перший погляд. Йдеться про несформованість загальної теорії національної безпеки, а отже і базового висхідного алгоритму будови понятійного апарату. На цю обставину звертало увагу багато дослідників, тому ми лише акцентуємо увагу на тій обставині, що формування понятійного апарату інформаційної безпеки є неможливим без формування даного апарату в рамках загальної теорії національної безпеки «національбезпекознавс-тво», як пропонує називати дану теорію український дослідник В.А.Ліпкан™. На цю ж обставину також звертають увагу чисельні дослідники проблем національної безпеки України[77].

Більш того, його формування має бути обумовлено та корелювати із останнім. Не можна, наприклад, визначати інформаційну

[76] *Ліпкан В А. Теоретичні основи та елементи національної безпеки України: Монографія. - К.: Текст, 2003. - 600 с; Ліпкан ВА., Ліпкан О.С., Яковенко О.О. Національна і міжнародна безпека у визначеннях та поняттях. - К.: Текст, 2006. - 256 с*

[77] *Бодрук О.С. Структури воєнної безпеки: національний та міжна родний аспекти / Рада національної безпеки і оборони України; Націо нальний ін-т проблем міжнародної безпеки. - К. : НІПМБ, 2001. - 300 с; Костенко Г.Ф. Теоретичні аспекти стратегії національної безпеки. Навчальний посібник. - К. : ЗАТ Видавничий дім «ДЕМІД», 2002. - 144 с; Данільян О.Г., ДзъобанъО.П., Панов М.І. Національна безпека України: структура та напрямки реалізації: Навчальний посібник. - Х.: Фоліо, 2002. - 285 с; Левицька М.Б. Теоретико-правові аспекти за безпечення національної безпеки органами внутрішніх справ України Дис...кандидата юрид. наук: 12.00.01. / Національна академія внутріш ніх справ України. - К., 2002. - 206 с; Мунтіян В.І. Економічна безпека. - К., 1999. - 464 с; Нижник Н.Р., Ситник Т.П., Білоус В.Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): Навчальний посібник / За заг. ред. П.В.Мельника, Н.Р.Нижник. - Ір пінь, 2000. - 304 с*

безпеку, використовуючи формулу: захищеність від..., у той час, як поняття національної безпеки (тобто родового поняття) визначається через формулу: управління загрозами та небезпеками. Зрозумілим є той факт, що понятійний апарат відповідних теорій, які слугують інструментом пізнання тих чи інших явищ у конкретних сферах життєдіяльності, не може розвиватися синхронно. Втім, фундаментальні принципи його формування мають бути дотримані. За інших умов казати про формування загальної теорії національної безпеки, а в її межах приватних теорій національної безпеки, зокрема теорії інформаційної безпеки, а отже й науково обґрунтованої цілісної концепції забезпечення національної безпеки стає неможливим.

На сьогодні саме інформаційні війни становлять найбільшу небезпеку нормальному функціонуванню системи національної безпеки. Події січня 2006 року з постачанням газу в Україну супроводжувалися застосуванням прийомів та засобів інформаційної війни Росією, про що було офіційно заявлено посадовими особами, що відповідають за забезпечення безпеки країни. Саме це й обумовлює детальний розгляд нами питань щодо визначення поняття та встановлення сутнісних ознак інформаційної війни.

Вперше термін «інформаційна війна» було введено у 1985 р. у Китаї[78]. В основі теоретичних підходів китайських спеціалістів в області інформаційного протиборства лежать погляди давньокитайського воєнного діяча Сунь-цзи. Він першим узагальнив досвід інформаційного впливу на супротивника. В трактаті «Мистецтво війни» Сунь-цзи писав: «у будь-якій війні, як правило, найкраща політика зводиться до захоплення держави в цілому... Одержати сотні перемог у бою - це не межа мистецтва. Підкорити супротивника без бою - ось це венець мистецтва»[79].

[78] *Кокошин АЛ, О системе стратегического управления в КНР // Вопросы, стратегического руководства обороной России. Краткий очерк. М.: ИПМБ РАН. 2001. - С. 36 - 38.*

[79] *Сунь цзы Искусство войны. - Ростов-на-Дону: Феникс, 2002. - 288 с.*

самим простим прикладом проведення інформаційної операції є той факт, що ви, шановний читач, у переважній більшості підручників та інших наукових і публіцистичних джерелах знайдете іншу інформацію: начебто, вперше термін *«інформаційна війна»* з'явився у наш час наприкінці 80-х років XX століття. Він став результатом плідної праці теоретиків збройних сил США та став уживаним після вдало проведеної роботи по знищенню СРСР[80]. Активного застосування даний термін набув під час проведення воєнної компанії США в Іраку у 1991 році, де вперше були не лише застосовані інформаційні технології, а вперше було відверто наголошено на цьому, що спричинило ще більший резонанс[8'].

Ось така пропаганда усього американського із використанням звичайних інформаційних важелів:

1) перші увели термін «інформаційна війна» (насправді першим це зробили китайці; інформаційний важіль - наукові, а скоріше, псевдо наукові статті та публікації);

2) перші полетіли в космос (насправді першим був СРСР; інформаційний важіль: друкована продукція американськими та прозахідними агентствами друку);

3) лише завдяки США СРСР виграв Велику вітчизняну війну (лише завдяки волі і героїзму радянського народу; інформаційний важіль: художній фільм «Спасіння рядового Райана»);

4) героїчно виграли війну у В'єтнамі (насправді ганебно її програли: інформаційний важіль: художній фільм «Рембо») тощо.

І таких міфів можна навести багато. Головне, це розуміння сутності і вагомості інформаційної зброї, її здатності змінювати світогляд людини, тобто знищувати душу, не руйнуючи тіло.

Передусім, коли йдеться про будь-яку війну, включаючи інформаційну, то слід говорити про певний стан взаємовідносин

[m] www.niss.gov.ua

[SI] *Литвиненко О.В. Спеціальні інформаційні операції. - К.: Рада національної безпеки і оборони України; Національний ін-т стратегічних досліджень, 1999. - 163 с*

між супротивниками. Здебільшого це не є присутнім, тому застосування даного терміну носить псевдонауковий характер. Для того, щоб детально розібратися у згаданому питанні, слід проаналізувати суспільні відносини в інформаційній сфері, згрупувати за певними ознаками ті з них, які можуть утворювати окремі явища, і вже потім застосовувати термінологію для означення і опису цих явищ за допомогою відповідної термінології.

Інформаційна війна виникає з нових підходів до застосування інформації, визначення її ролі та місця. Можна виділити два трактування поняття інформаційної війни: *гуманітарну і технічну.*

Наприклад, М. Павлютенкова зазначає, що у гуманітарному сенсі інформаційна війна становить собою активні методи трансформації інформаційного простору, що знаходить свій вираз у системі нав'язування моделей світу, які покликані забезпечити бажані типи поведінки, атаках на структури породження інформації - процеси міркувань. У той же час технічне трактування даного поняття полягає у тому, що за допомогою спеціальних програм руйнується обладнання, програмне забезпечення тощо*-'.

Отже, аналіз даного бачення певних процесів в інформаційній сфері дозволяє казати про підміну понять, адже війна за своїм значенням означає стан, у якому держави застосовують одна проти одної усі форми тиску з дотриманням дії законів та звичаїв ведення війни *(jus in bello)*[S3]. Втім, наведений вище приклад бачення поняття інформаційної війни дає усі підстави стверджувати, що описані вище ознаки не складають даного поняття.

Безперечним є той факт, що формування інформаційного суспільства стає не лише фактом, а все більше починає впливати на формування державної політики інформаційної безпеки. Досяг-

[82] *Павлютенкова М. Информационная война -реальная угроза или современный миф? /І Власть. - 2001. - № 12. - С. 19 - 23.*

[83] *Юридична енциклопедія: В 6 т. / Редкол.: Ю.С. Шемшученко (відп. ред.) та ін.- К.: Українська енциклопедія ім. МЛ.Бажана, 1998. Т.l: АГ. - С. 455.*

нення тих чи інших цілей виявилося можливим із застосуванням лише інформаційних технологій, які б чинили вплив на суспільну свідомість. Одним з проявів застосування даного методу є сильний часовий пресинг на суб'єктів державного управління, який не залишає їм часу на прийняття виваженого, такого, що відповідає національним інтересам рішення. Відтак, досягнення певних геополітичних та інших важливих цілей уможливлюється за допомогою невійськових методів.

Сумний досвід неприділення належної уваги даним питанням спричинив до розпаду СРСР, могутньої держави, яка до 1991 року разом із США утворювали біполярну систему світу. Саме це дає можливість погодитись із *Логіновим О.В.,* який пропонує розробити *концепцію інформаційного стримування.*

Нині відсутня розроблена на концептуальному рівні концепція (система теоретико-методологічних засад, положень) забезпечення інформаційної безпеки. Більш того, аналіз сучасної геополітичної обстановки і безпекотрансформаційних процесів дозволяє зробити висновок, що проти України здійснюються широкомасштабні інформаційні акції, спрямовані на дискредитацію, дезорганізацію, підрив іміджу, інформаційну кластери-зацію і дестабілізацію нашої держави. І, передусім, цей вплив чиниться на систему державного управління.

Зазначимо, що четверта влада - ЗМІ - відіграла значну роль в укоріненні у свідомості пересічного громадянина терміну «інформаційна війна». При чому під останнім ЗМІ як правило розуміють використання компромату через засоби масової інформації, здебільшого електронні. Ідеальним засобом для цього є Інтернет, який дає можливість розповсюджувати будь-яку інформацію без будь-яких обмежень.

Що стосується іншого розуміння - технічного - то тут обов'язковою умовою є те, що ведення інформаційної війни є результатом узгодженої діяльності з використання інформації як зброї ведення бойових дій у будь-якій сфері життєдіяльності. При цьому *інформаційна війна* включає наступні дії:

• *здійснення впливу на інфраструктуру систем життєзабезпечення* - телекомунікації, транспортні мережі, електростанції тощо;

• *промисловий шпіонаж* - порушення прав інтелектуальної власнбсті, розкрадання патентованої інформації, викривлення або знищення важливих даних, проведення конкурентної розвідки;

• *хакінг* - злам і використання особистих даних, ідентифікаційних номерів, інформації з обмеженим доступом тощо[1]".

Коли йдеться про інформаційну війну, то слід говорити про існування рішучої і небезпечної діяльності, пов'язаної із реальними бойовими діями. Більш того, за даного випадку постає необхідність у виокремленні декількох підвидів інформаційних війн: кібернетична війна, електронна війна, психотронна війна, психотропна війна, штабна війна, психологічна, енергоінформа-ційна війна.

Таке розуміння інформаційної війни надає можливість погодитись із визначенням поняття інформаційної війни, яке міститься у керівних документах збройних сил США.

Згідно з Доктриною проведення інформаційних операцій **інформаційна війна** - дії, що вчинюються для досягнення інформаційної переваги у підтримці національної воєнної стратегії через вплив на інформацію та інформаційні системи супротивника при одночасному забезпеченні безпеки власної інформації і інформаційних систем[5]. Одним з прикладів є існування спеціальної програми запису всіх телефонних дзвінків, що виходять за кордон США на спеціальну апаратуру. За допомогою даної програми всі телефонні дзвінки, що виходять за межі країни записуються, а потім пропускаються через спеціальний пристрій,

" *Павлютенкова М. Информационная война -реальная угроза или современный миф? І/ Власть. - 2001. - № 12. - С. 19 - 23.*

[85] www.pccip.gov

який за допомогою пошукових систем за ключовими словами здійснює виявлення та ідентифікацію важливої інформації.

Відтак, існування розвиненої системи інформаційної безпеки закладе фундамент для стійкого функціонування системи національної безпеки. На думку деяких дослідників, стрімкий розвиток інформаційних технологій спричинить у майбутньому появу нових за змістом видів війн, які відбуватимуться без жодного пострілу. Особливо наголосимо, що сучасні інформаційні війни спрямовані здебільшого на дезорієнтацію людини, зміну її світогляду, підмінну цінностей і перетворення на інформаційного споживача, тобто інформаційного раба.

Цілі інформаційної війни є дещо іншими, аніж війни у звичному розумінні. Якщо за умов ведення *звичайної війни,* головною метою є фізичне знищення противника та ліквідація його збройних сил, то за умови ведення *інформаційної війни* відбувається широкомасштабне порушення роботи фінансових, транспортних і комунікаційних мереж і систем, руйнування економічної інфраструктури і підкорення населення країни, що зазнала атаки, зміни світоглядних настанов, зародження сумніву в необхідності та доцільності існування в рамках самостійної, суверенної держави.

У рамках досліджуваних проблем, доцільним є проведення компаративного аналізу понять «інформаційна війна» і «інформаційне протиборство», з метою виокремлення ознак, що споріднюють і різнять їх.

На сьогодні термін «інформаційна війна» використовується у двох площинах:

- у широкому розумінні - для визначення протиборства в інформаційній сфері в засобах масової інформації для досягнення різних політичних цілей;
- у вузькому розумінні - для визначення воєнного протиборства, у військовій інформаційній сфері для досягнення односторонніх переваг в отриманні, зборі, обробці та використанні інформації на полі бою (в операції, битві).

У вітчизняній практиці в широкому розумінні частіше використовують термін «інформаційна протиборство» у вузькому розумінні - «інформаційні воєнні дії».

Інформаційне протиборство - це форма боротьби сторін в інформаційному просторі з використанням політичних, економічних, дипломатичних, військових та інших методів, способів та засобів, для впливу на інформаційне поле супротивника та захисту власного інформаційного поля в інтересах досягнення поставлених цілей.

Ураховуючи дане визначення можна зазначити, що інформаційне протиборство включає в себе три незмінні складові: 1) вплив; 2) аналіз; 3) безпосереднє протиборство.

Основним елементом, від якого залежить ефективність компанії, є аналіз, мета якого полягає в оцінці, стратегічному прогнозуванні та плануванні в аспектах внутрішньополітичного та зовнішньополітичного становища. Що ж стосується «інформаційної війни» то, як всеохоплююча, цілісна стратегія, вона обумовлена все зростаючою значимістю та цінністю інформації у питаннях командування, управління та політики. Також можна послуговуватись визначенням «інформаційної війни» як «комунікативної технології по впливу на масову свідомість з короткочасними та довготривалими цілями».

На Заході інформаційну війну визначають як «нефізичну атаку на інформацію, інформаційні процеси та інформаційну інфраструктуру», причому «ціллю інформаційної війни є вплив на систему знань та уявлень зовнішнього супротивника». Під *знанням* тут розуміється об'єктивна інформація, загальна для усіх, а під уявленнями - інформація, яка носить суб'єктивний характер. Основним інструментом ведення інформаційної війни є *інформаційна зброя.*

До «інформаційної зброї» ми будемо відносити, по-перше, засоби інформаційно-технічного характеру, які знищують, перекручують або викрадають інформацію, не зважаючи на систему захисту, обмеження доступу до цієї інформації законних

користувачів. По-друге, це безперечно, інформаційно-психологічні засоби, які дезорганізують інформаційні системи, шляхом дезінформації, формування помилкових логічних інформаційних концепцій, інтерпретацій та ін., впливаючи, таким чином, на суспільну думку, на життя суспільства, держави або групи держав в цілому.

Таким чином, **інформаційна зброя** - це пристрої та засоби, які призначені для нанесення протидіючій стороні максимальної шкоди в ході інформаційної боротьби (шляхом небезпечних інформаційних впливів).

Об'єктами впливу можуть бути: *інформаційно-технічні* системи, які включають людину, *інформаційно-аналітичні* системи, які включають людину, *інформаційні ресурси,* системи формування суспільної свідомості та думки, яка базується на засобах масової інформації та пропаганди, а також психіки людини.

Інформаційна зброя - інструмент встановлення контролю над інформаційними ресурсами потенційного супротивника, тому інформаційна зброя втручається в роботу систем управління та інформаційних систем, систем зв'язку та ін., у цілях порушення їх працездатності, аж до повного виведення їх з ладу, вилучення, перекручення даних, які в них містяться, або цілеспрямованого введення спеціальної інформації. Подеколи інформаційна зброя виступає в ролі розповсюджуваної дезінформації в системі формування суспільної свідомості й прийняття рішень.

Також до інформаційної зброї включають і сукупність спеціальних способів та засобів впливу на психіку суспільства та держави в цілому.

Для проведення будь-якої інформаційної компанії як в міжнародних відносинах, так і на внутрішньому інформаційному полі слід ураховувати особливості конкретного інформаційного простору. На початку необхідно розшукати вразливі точки в інформаційному просторі і лише згодом переходити до рішучих дій.

Інформаційна зброя повинна враховувати варіанти протидії і чим більше варіантів протидії враховано, тим більше імовірності

успіху в той чи іншій інформаційній агресії. Також необхідно підкреслити, що специфікою інформаційної війни (як форми інформаційного протиборства) є те, що вона ведеться, на відміну від збройної боротьби як у мирний, так і у воєнний час. Вона націлена на всі можливості та фактори ураженості, які неминуче виникають при зростанні залежності від інформації, а також на використання інформації у найрізноманітніших конфліктах. Об'єктом уваги стають інформаційні системи (включаючи відповідні лінії передач, центри обробки та людський фактор цих систем), а також інформаційні технології, які використовуються в системах озброєння. Таким чином, можна виділити наступні *сфери інформаційного протиборства:* політична, дипломатична, воєнна, технологічна, соціальна, ідеологічна.

Інформаційна війна має наступальні та оборонні складові, але, починаючи з цільового проектування та розробки своєї архітектури командування, управління, комунікації, комп'ютерів та розвідки, яка забезпечує особам, які приймають рішення, відчутну інформаційну перевагу у різноманітних конфліктах. Інформаційна війна може бути спрямована проти *трьох елемен тів:* комп'ютер; програмне забезпечення; людина.

Однією з головних цілей інформаційної війни є подавления в людині морального творчого початку.

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

Взагалі ж технології інформаційної ери певним чином зрівняли індустріальні, постіндустріальні та доіндустріальні країни: всі вони мають доступ до інструментарію, необхідного для ведення інформаційної війни, а отже, і виступають як суб'єктами, так

об'єктами інформаційної війни, а отже і забезпечення інформаційної безпеки.

2. Поняття та зміст інформаційного протиборства

Інформаційне протиборство - суперництво соціальних систем (країн, блоків країн) в інформаційній сфері з приводу впливу на ті або інші сфери соціальних відносин і встановлення контролю над джерелами стратегічних ресурсів, у результаті якого одна група учасників суперництва отримує переваги, необхідні їм для подальшого розвитку.

За інтенсивністю, масштабами та засобами, які використовуються, виділяють наступні *ступені інформаційного протиборства:* інформаційна експансія, інформаційна агресія та інформаційна війна.

Інформаційна експансія — діяльність із досягнення національних інтересів методом безконфліктного проникнення в інформаційну сферу з метою:

• поступової, плавної, непомітної для суспільства зміни системи соціальних відносин за зразком системи джерела експансії;

• витіснення положень національної ідеології і національної системи цінностей і заміщення їх власними цінностями й ідеологічними установками;

• збільшення ступеня свого впливу та присутності, встановлення контролю над стратегічними інформаційними ресурсами, інформаційно-телекомунікаційною структурою і національними ЗМІ;

• нарощування присутності власних ЗМІ в інформаційній сфері об'єкта проникнення і т.п.

Інформаційна агресія - незаконні дії однієї зі сторін в інформаційній сфері, спрямовані на нанесення супротивнику конкретної, відчутної шкоди в окремих областях його діяльності шляхом обмеженого та локального по своїх масштабах застосування сили.

О.шаки інформаційної агресії:

1) виключення із засобів інформаційної дії самих небезпечних видів, що не дозволяють надійно контролювати розміри, завдається збитку - інформаційної зброї;

2) обмеження розмірів простору, об'єктів інформаційної інфраструктури та соціальних груп, що піддаються ураженню інформаційною дією (агресія зачіпає інформаційний простір де-ржави-жертви не цілком, а тільки його частину);

3) обмеження за метою (переслідує локальну, приватну мету) і часу (як правило, агресія припиняється після повного досягнення агресором усієї поставленої конкретної мети й рідко набуває затяжного характеру), а також по силах і засобах, що залучаються.

Інформаційна війна - найвищий ступінь інформаційного протиборства, спрямований на розв'язання суспільно-політичних, ідеологічних, а також національних, територіальних та інших конфліктів між державами, народами, націями, класами й соціальними групами шляхом широкомасштабної реалізації засобів і методів інформаційного насильства (інформаційної зброї).

Можна вважати, що в інформаційній сфері агресія переростає у війну в тому випадку, якщо одна зі сторін конфлікту починає широко застосовувати проти своїх супротивників інформаційну зброю. Цей критерій дозволяє виділити з усього різноманіття процесів і явищ, що відбуваються в інформаційному суспільстві такі, які представляють для його нормального (мирного) розвитку найбільшу небезпеку.

Нині відсутні міжнародні та національні правові норми, які дозволяють в мирний час (за відсутності офіційного оголошення війни з боку агресора) юридично кваліфікувати ворожі дії іноземної держави в інформаційній сфері, що супроводжуються нанесенням збитку інформаційній або іншій безпеці країни, як акції інформаційної агресії або інформаційної війни. Крім того, відсутні чіткі, однозначні, закріплені юридично критерії оцінки

отриманого в результаті інформаційної агресії або інформаційної війни матеріального, морального, іншого збитку. Це дозволяє в мирний час активно використовувати самий небезпечний і агресивний арсенал сил і засобів інформаційної війни - як основний засіб досягнення політичної мети.

Беззаперечним лідером на шляху впровадження в практику концепції інформаційного протиборства є США. Досить сказати, що витрати, в цій країні на реалізацію даної концепції до 2005р., становлять понад 17 млрд доларів. Концепція інформаційного протиборства США на воєнному рівні була покладена в основу при розробці аналогічних концепцій провідних західних країн, а також керівних документів НАТО по цих питаннях. Тому у зв'язку з обмеженістю часу доцільно більш детально розглянути саме цю концепцію.

Розроблена в США концепція інформаційного протиборства передбачає його ведення на воєнному та державному рівнях. На державному рівні метою інформаційного протиборства є послаблення позицій конкуруючих держав, підрив їх національно-державних основ, порушення системи національного управління за рахунок інформаційного впливу на політичну, дипломатичну, економічну та соціальну сфери життєдіяльності країни, проведення психологічних операцій, підривних та інших деморалі-зуючих пропагандистських акцій. Воно спрямовано на забезпечення національних інтересів США, упередження міжнародних конфліктів, терористичних акцій, забезпечення інформаційної безпеки країни. Воно розглядається як вид стратегічного протиборства країн.

За висновками аналітиків американської корпорації «Ренд» воно передбачає вирішення наступних задач:

- створення в країні противника атмосфери бездуховності, негативного відношення до культурної спадщини;
- маніпулювання суспільною свідомістю і політичною орієнтацією груп населення держави з метою створення політичної напруги і хаосу;

- дестабілізація політичних відношень між партіями, об'єднаннями та рухами з метою провокації конфліктів, розпалення недовіри, підозрілості, загострення політичної боротьби, провокування репресій проти опозиції і навіть громадянської війни;
- зниження рівня інформаційного забезпечення органів влади й управління, ініціація помилкових управлінських рішень;
- дезінформування населення про роботу державних органів, підрив їх авторитета, дискредитація органів управління;
- провокування соціальних, політичних, національних і релігійних зіткнень;
- ініціювання страйків, масових заворушень та інших акцій економічного протесту;
- ускладнення прийняття органами управління важливих рішень;
- підрив міжнародного авторитету держави, її співробітництва з іншими країнами.

Основними *формами інформаційного протиборства* на державному рівні є:

- політичні, дипломатичні й економічні акції;
- інформаційні та психологічні операції;
- підривні та деморалізуючі пропагандистські дії;
- сприяння опозиційним і дисидентським рухам;
- надання усебічного впливу на політичне і культурне життя з метою розвалу національно-державних підвалин суспільства;
- проникнення в систему державного керування.

На воєнному рівні доцільно використовувати термін інформаційна боротьба за аналогією радіоелектронна боротьба, психологічна боротьба. Інформаційна боротьба визначається як комплекс заходів, які провадяться в масштабах ЗС для досягнення інформаційної переваги над противником шляхом впливу на інформацію, якою він володіє, процеси, що залежать від інформації, інформаційні системи, комп'ютерні мережі з одночасним захистом від аналогічних впливів з боку противника. Виділяються наступальна й оборонна складові інформаційної боротьби. Крім

того, перед ЗС вперше поставлене завдання впливу на противника ще в загрозливий період з тим, щоб забезпечити вигідний для США напрямок процесів управління і прийняття рішень протилежною стороною.

Отже, ***основним завданням інформаційної боротьби*** є:

- отримання розвідувальної інформації шляхом перехоплення та розшифрування інформаційних потоків, що передаються по каналам зв'язку, а також по побічним випромінюванням, а також за рахунок спеціального втілення технічних засобів перехоплення інформації;
- отримання потрібної інформації шляхом перехоплення й обробки відкритої інформації, що передається через незахищені канали зв'язку, циркулює в інформаційних системах, а також опублікованої у відкритих джерелах та ЗМІ;
- електромагнітний вплив на елементи інформаційних і телекомунікаційних систем;
- психологічний вплив, спрямований проти персоналу та осіб, що приймають рішення;
- формування і масоване розповсюдження через інформаційні канали противника та глобальні мережі дезінформації та тенденційної інформації;
- вогневе придушення (у воєнний час) елементів інфраструктури державного і воєнного управління;
- здійснення несанкціонованого доступу до інформаційних ресурсів з подальшим їх викривленням, знищенням або викраденням, або порушенням нормального функціонування таких систем;
- захист від аналогічних впливів з боку противника.

Новизна американського підходу полягає в комплексному використанні різнорідних сил для досягнення глобальної мети - інформаційної переваги.

Для реалізації розробленої в США концепції ***інформаційного протиборства*** на воєнному і державному рівнях виділяються ***шість основних складових:***

1) боротьба із системами управління супротивника (command and control warfare),

2) боротьба на основі розвідувальних технологій (intelligence-based warfare -IBW), електронна боротьба (electronic warfare),

3) психологічна боротьба (psychological warfare),

4) економічна інформаційна боротьба (economic information warfare - EW),

5) кібернетична боротьба (cyberwar);

6) боротьба з використанням хакеров (hackerwar).

Дамо коротку характеристику деяким з них.

Боротьба на основі розвідувальних технологій (intelligence-based warfare - IBW) - полягає в зібранні та розподіленні розвідувальної інформації від датчиків у реального або близькому до реального часу для керування бойовими діями та наведення зброї. За оцінкою американських експертів технологія, що дозволяє за допомогою технічних засобів зібрати (перехопити) і об'єднати всі сигнали, що надходять, виділити серед них корисні і направити їх відповідному споживачеві, з'явиться в найближчі десять років. Нова система збору і розподілу інформації, об'єднаної на глобальному рівні, повинна забезпечити оптимальні можливості для взаємодії видів і родів військ і навіть збройних сил різних країн.

Психологічна боротьба, що складається з організації і проведення різних психологічних операцій.

1. Операції проти волі нації (operations againsts the national will).

2. Операції проти командування супротивника (operations againsts opposing commanders).

3. Операції проти ворожих військ (operations against troops).

4. Операції на рівні національних культур (cultural conflict).

Сполучення засобів економічної й інформаційної боротьби (economic information warfare) може являти собою дві форми - інформаційну блокаду й інформаційний імперіалізм. При цьому під інформаційним імперіалізмом розуміється монопольне володіння

значною частиною інформаційних ресурсів і домінування з елементами диктату на ринку інформаційних послуг. Інформаційна блокада полягає у припиненні або скороченні обсягів доступу однієї країни до інформаційних ресурсів іншої, що може вплинути на її економічне становище або навіть призвести до кризової ситуації.

Кібернетична боротьба - це боротьба в кібернетичному (віртуальному) просторі - просторі комп'ютерно-телекомунікаційних мереж. Вона ведеться спеціально створеними підрозділами з використанням широкого спектра засобів, включаючи моделювання й імітацію військових дій.

Особливу групу представляють хакери - комп'ютерні злам-ники, що практикуються на проникненні в чужі комп'ютерні системи.

Для вирішення завдань інформаційного протиборства створюються відповідні органи управління, сили та засоби. Так, у ЗС США керівництво захистом інформаційної інфраструктури покладено на управління інформаційних систем МО. Для організації та ведення наступальних заходів ІБ усі види ЗС мають власні центри. Центр ІБ сухопутних військ (LIWA), створений у 1994 році, знаходиться у форті Белвуар (штат Вірджинія). Аналогічний центр ВМС (NIWA), також створений у 1994 р., знаходиться у форті Мід (штат Меріленд). Центр ІБ Військово - Повітряних Сил (AFIWC), створений ще раніше в 1993 р., знаходиться на авіабазі Келі (м. Сан-Антоніо, штат Техас). Дії цих центрів координуються створеним у січні 1995 р. центральним органом МО США - виконавчим комітетом з питань ІБ (Information Warfare Executive Board), головне завдання якого полягає в прискоренні «розроблення та досягнення цілей ІБ». Аналогічні структури створюються і в стратегічних об'єднаннях. Продовжується також розвиток органів ІБ і по вертикалі.

Структури психологічних операцій в США створені у межах ЦРУ та МО, а саме в об'єднаному командуванні спеціальних операцій. Принципові рішення з питань проведення психоло-

гічних операцій приймає воєнно-політичне керівництво США в особі президента, уряду та Конгресу. Президент як верховний головнокомандувач здійснює загальне керівництво психологічними операціями через раду національної безпеки та міністерство оборони, а оперативне керівництво через Комітет начальників штабів.

Загальну організацію та планування психологічних операцій в збройних силах США здійснює міністерство оборони через апарат помічника міністра оборони з спеціальних операцій та конфліктів низької інтенсивності, який керує діяльністю всіх відповідних органів та формувань через міністерства та штаби видів збройних сил. Кожний вид збройних сил США має в об'єднаному командуванні спеціальних операцій власні сили та засоби психологічних операцій, однак найбільша їх частина (близько 85%) зосереджена в сухопутних військах. У командуванні спеціальних операцій сухопутних військ сформоване командування по роботі з цивільним населенням та психологічним операціям, яке утворене широко відомою 4-ою групою психологічних операцій та 96-м батальйоном по роботі з цивільним населенням, підрозділи яких сьогодні приймають безпосередню участь у війні з Іраком.

Для вирішення завдань інформаційного протиборства на державному рівні також широко залучаються ЦРУ, інші спеціальні служби, створюються нові структури. Так, згідно з директивою президента США PDD-68 у 1999 році була створена нова структура під назвою Міжнародна група суспільної інформації (International Public Information Group), відома як IPI. Задачами цієї організації є професійне використання розвідувальної інформації з метою створити вплив на емоції, мотиви, поведінку іноземних урядів, організацій та окремих громадян.

Налагоджену систему психологічних операцій мають не тільки провідні, а також суміжні з Україною держави, такі як Румунія, Польща, Туреччина. Вже сьогодні вони за складом, технічним оснащенням та чисельністю здатні застосовувати як

традиційні, так і новітні форми інформаційно-психологічного впливу.

У Війську Польському задачі надання інформаційно-психологічного впливу на війська і населення супротивника для досягнення політичних, військових і пропагандистських цілей покладені на центральну групу психологічних дій (ЦГПД) (Centraliia Grupa Dzialan Psychologicznych, місце дислокації м. Бидгощ). Центральна група психологічних дій складається з керування (штабу), а також з інформаційно-аналітичних, теле- і радіомовних, редакційно-видавничих і тилових підрозділів. Особовий склад лише кадровий. Середній вік польських фахівців психологічних операцій 32 роки. Більшість з них володіє декількома іноземними мовами, у тому числі англійським - не менш 75% військовослужбовців. Практично весь командний склад стажувався в структурах психологічних операцій натовських армій, має досвід роботи в штабах об'єднання збройних сил альянсу різного рівня, брав участь у миротворчих операціях. Відповідно до планів генерального штабу щодо подальшої реорганізації ЗС Польщі на 2003-2008 роки, передбачається включити ЦГПД до складу національних сил спеціальних операцій, які планується сформувати, а на основі її керівного складу створити в структурі ГШ управління психологічної боротьби.

До останнього часу Росія не мала власної державної концепції з проблем інформаційного протиборства. Деякі російські фахівці вважають, що саме її відсутність була одним із факторів розпаду СРСР і поразки у «холодній війні».

«Доктрина інформаційної безпеки Росії» була підписана президентом Російської Федерації лише у вересні 2000 року. її головною особливістю є врахування інтересів трьох основних об єктів національної безпеки: особи, суспільства та держави.

Забезпечення інформаційної безпеки та впровадження основних положень Доктрини здійснюється Управлінням інформаційної безпеки при Раді безпеки РФ. її експерти вважають, що для забезпечення інформаційної безпеки Російської Федерації необ-

хідно створення особливого координаційного органу, який матиме право контролювати розробку і застосування інформаційної зброї, а також міжвідомчого аналітичного центру з проблем інформаційно-психологічних технологій на базі ФСБ, МВС, ЗС та Ради безпеки РФ.

Таким чином, в концепціях національної безпеки багатьох провідних країн світу визначено, що головною рисою нового століття буде перенесення акцентів у галузь інформаційного протиборства, а досягнення інформаційної переваги стає обов'язковою умовою перемоги над будь-яким противником.

Досвід проведення останніх локальних війн і збройних конфліктів в Югославії, Афганістані, Іраку показав неминучість і високу ефективність заходів інформаційної боротьби.

З огляду на це, прогнозується подальше зростання ролі інформаційних та психологічних операцій в забезпеченні національних інтересів провідних країн світу. За оцінками експертів інформаційна зброя є одною з головних загроз інформаційній безпеці держави. На сьогодні вже більше 20 країн планують і здійснюють різноманітні інформаційні операції. А сумарні витрати на розробки в галузі інформаційної зброї перевищують 120 млрд доларів на рік.

3. Форми і засоби ведення інформаційної боротьби

Сьогодні інформаційна боротьба (ІБ) в Україні знаходиться на стадії становлення. її сутність ще продовжує корегуватись та розвиватись, що можливо призведе в недалекому майбутньому до появи зовсім інших уявлень і базових визначень. Складність ІБ обумовлена багатогранністю проявів інформації та інформаційних процесів. Подальший розвиток інформаційної боротьби наприкінці XX сторіччя пов'язаний зі змінами в галузі інформаційних технологій та зростанням ролі інформації в усіх сферах життєдіяльності суспільства і держави. В збройних силах провідних країн світу інформаційна боротьба трансформується

в окремий інтегрований вид стратегічного (оперативного) забезпечення операцій а в подальшому як окремий вид боротьби. Відповідно з'являються нові форми ведення інформаційної боротьби: інформаційна операція, спеціальна інформаційна операція.

Для аналізу сучасних форм ведення інформаційної боротьби розглянемо документи США «JOINT DOCTRINE **FOR INFORMATION** OPERATIONS (Joint Pub 3-13)». «Об'єднана доктрина інформаційних операцій» визначає основні цілі інформаційної боротьби, об'єкти на які спрямований інформаційний вплив, та форми ведення інформаційної боротьби. Зрозуміло, що інформаційна операція це комплексна форма ведення інформаційної боротьби, яка змінюється в часі відповідно фазам розвитку подій і складається з декількох взаємопов'язаних складових.

Другий висновок - інформаційна боротьба ведеться не тільки в ході військового конфлікту, але ж ще задовго до його початку та після завершення. На етапі підготовки до збройної боротьби заходи інформаційної боротьби проводяться в першу чергу на державному рівні з метою створення бажаних воєнно-політичних та економічних умов для початку агресії. З іншого боку, вона є ефективним засобом запобігання і стримування військових конфліктів. До основних особливостей ведення інформаційної боротьби в цей період можна віднести: обмеженість у використанні сил, способів і засобів інформаційного впливу на противника; дотримання існуючих норм міжнародного права, тісну взає-модію силових відомств та інших державних структур при проведенні заходів інформаційної боротьби. З початком військових (бойових) дій сили і засоби інформаційної боротьби вирішують завдання з використанням їх усього можливого арсеналу, включаючи знищення об'єктів інформаційної інфраструктури противника.

Після досягнення воєнно-політичної мети інформаційна боротьба спрямована на: стабілізацію соціально-політичної обстановки в країні противника; нейтралізацію осередків опору; лояльне ставлення до перетворень в країні світової спільноти.

Інформаційна боротьба набуває активного стратегічного характеру, ведеться без обмежень у просторі та часі та характеризується економічною доцільністю, нелетальністю дії та високою ефективністю щодо досягнення воєнно-політичної мети.

Актуальне питання для інформаційної безпеки України це можливе проведення проти неї інформаційної операції. У вказаному документі (Joint Pub 3-13) наступальна інформаційна операція складається:

1. Operations Security (OPSEC) - Захист інформації про план операції, про елементи, які суттєво впливають на досягнення успіху, про союзні сили, аби таким чином уповільнити процес прийняття рішення противником. (JP 3-54 «Joint Doctrine for Operations Security»)

2. Military deception - введення в оману. Використання усіх можливих засобів для введення в оману противника стосовно ходу операції, ключових точок місцевості, напрямків основних зусиль. Уповільнює процес прийняття рішення противником через його системи збору і аналізу інформації. (JP 3-58 «Joint Doctrine for Military Deception»)

3. Electronic Warfare (EW) - РЕБ. Використання спрямованої електромагнітної енергії для впливу на противника та захист власних радіосистем. (JP 3-51 «Electronic Warfare in Join Military Operations»).

5. Physical attack / destruction. Атака та фізичне знищення. Використання зброї проти визначених цілей для досягнення більшої ефективності інформаційної операції.

6. Computer network attack (CNA) - Атака на комп'ютерні мережі.

7. Psychological Operations (PSYOP) — психологічні операції. Забезпечують умови для відновлення порядку, підтримку дружньо налаштованого населення. Вплив на противника та нейтралізація психологічного впливу з його боку. Психологічні операції повинні підтримувати заходи по введенню противника в оману. (JP 3-53 «Doctrine for Joint Psychological Operations»),

8. Public Affairs (PA) - Суспільні відносини. Інформування власної і іноземної аудиторії про свої цілі, дружні війська, хід операції. PA не використовують для введення в оману чи розповсюдження дезинформації. (JP 3-61 «Doctrine for Public Affairs in Joint Operations»).

9. Civil Affairs (CA) - цивільні відносини. Встановлення військовим командуванням дружніх стосунків з місцевими органами управління, населенням, місцевим лідерами в районі своїх інтересів. CA & PSYOP можуть бути поєднані. (JP 3-57 «Doctrine for Joint Civil Affairs»).

У мирний час, в умовах обмежень у використанні сил, способів і засобів кількість складових інформаційної операції зменшується до чотирьох. Computer network attack (CNA). Psychological Operations (PSYOP). Public Affairs(PA). Civil Affairs (CA). Це ті види інформаційного впливу, які несуть постійну загрозу інформаційній безпеці України. З них найбільш небезпечні - це атаки на комп'ютерні мережі та психологічні операції, в межах яких, як вважають фахівці, сформувався самостійний вид зброї - інформаційна зброя.

Відповідно до одного з існуючих визначень **інформаційна зброя** - це сукупність засобів і технологій, призначених для ведення інформаційної боротьби. За об'єктами впливу інформаційну зброю можна поділити на два основних класи:

1. Інформаційно-технічна зброя, що впливає на інформаційні ресурси, інформаційну інфраструктуру збройних сил, держави в цілому.

2. Інформаційно-психологічна зброя, що впливає на морально-психологічний стан людини, соціальних та інших груп населення, суспільства в цілому.

Інформаційна зброя може характеризуватись такими показниками, як цілеспрямованість, вибірковість, розосередженість, масштабність впливу, досяжність, швидкість доставки, комплексність впливу на людей, технічні засоби і системи, мож-

ливість регулювання (дозування) «потужності» впливу тощо. їй. притаманні такі особливості:

• скритність — можливість досягти мети без видимої підготовки та об'явлення війни;

• масштабність - можливість нанести непоправного збитку, не визначаючи національних кордонів та суверенітетів;

• універсальність - можливість багатоваріантного вико ристання як військовими, так і цивільними структурами краї ни, що нападає, проти військових і цивільних об'єктів країни, яка підлягає нападу;

• економічність - вигідне для атакуючої сторони співвідно шення витрат, необхідних на розробку засобів впливу, і одержу ваного при цьому ефекту, порівняного з очікуваною катастро фою для країни, яка підлягає нападу.

За своїми економічними показниками інформаційна зброя може бути віднесена до різновиду асиметричної зброї.

На сьогодні **інформаційно-технічна зброя** визначається як засоби знищення, викривлення або викрадання інформаційних масивів, видобування з них необхідної інформації після подолання системи захисту, обмеження або заборони доступу до них законних користувачів, дезорганізації роботи технічних засобів, виводу з ладу телекомунікаційних мереж, комп'ютерних систем, усіх засобів високотехнологічного забезпечення життя суспільства і функціонування держави.

Засоби несанкціонованого збору інформації дозволяють здійснити несанкціонований доступ до комп'ютерних систем, визначати коди доступу, ключі до шифрів чи іншу інформацію про запіифровані дані. До них відносяться програмні продукти типу «KNOWBOT» та «TRAP DOOR». Програмні продукти типу «KNOWBOT» (пошуковий робот) здатні переміщуватися в інформаційній мережі від комп'ютера до комп'ютера і при цьому розмножуватися, створюючи копії. Знайшовши цікавлячу його інформацію, «KNOWBOT» залишає в цьому місці свою копію, що збирає інформацію й у визначений час передає її. З метою виклю-

 чення виявлення в програмних продуктах такого типу можуть бути передбачені функції самопереміщення і самознищення.

Програмні продути типу «TRAP DOOR» (програми-пастки, програми-закладки) призначені для збору та передачі інформації про ключі даних та паролі. Вони, звичайно, вмонтовуються в програмні продукти широкого вжитку (офісні та сервісні програми, операційні системи, локальні модулі онлайнових комп'ютерних ігор тощо).

Створені і постійно модернізуються спеціальні технічні пристрої, що дозволяють зчитувати інформацію з моніторів комп'ютерів. Перспективним є також створення мініатюрних спеціалізованих комплексів збору, обробки і передачі інформації, що можуть впроваджуватися під виглядом звичайних мікросхем до складу всіляких радіоелектронних пристроїв.

Засоби перекручування і знищення інформації включають численні комп'ютерні віруси. Особливу небезпеку становлять останні різновиди вірусів типу «WORM», які, на відміну від звичайних вірусів, являють собою не закінчену програму, а набір стандартних команд операційної системи (сценарій), що значно ускладнює процеси їх знаходження та нейтралізації.

До *засобів порушення функціонування комп'ютерно-телекомунікаційних мереж* відносяться «Логічні бомби», «Бомби електронної пошти» - атаки на відмову в обслуговуванні (DoS attacks) і т.д.

Логічна бомба являє собою управляючу програму, що перебуває в неактивному стані до одержання команди на виконання визначених дій на зміну чи руйнування даних, а також порушення нормального функціонування інформаційно-обчислювальних систем. Бомби електронної пошти - це програми, що спричинюють різке зростання обсягу повідомлень електронної пошти з метою перевантаження серверів. Саме в такий спосіб був заблокований у березні 1999 р. на троє діб сервер НАТО. Невідомий адресат регулярно надсилав на адресу Північноатлантичного блоку близько 2000 телеграм на день, що переповнило елект-

ронну «поштову скриньку» серверу. Аналогічно діють атаки на відмову в обслуговуванні.

В окремий різновид програмно-технічної зброї відносяться програмні продукти типу «TROJAN IIORSE» (троянський кінь). Програмні продукти даного типу здатні відкривати повний доступ до цікавлячого комп'ютера при роботі в мережах різного типу.

Інформаційна зброя, як і інформаційна боротьба з розвитком суспільства та інформаційних технологій набули відповідних змін

На перспективу, враховуючи, що розвиток сучасної комп'ютерної техніки дійшов до створення штучного інтелекту, очікується поява «інтелектуальної» інформаційно-технічної зброї.

Відповідно з документами США психологічна операція є складовою інформаційної операції організується і проводиться згідно (JP 3-53 «Doctrine for Joint Psychological Operations») «Доктрини об'єднаних психологічних операцій».

Інформаційно-психологічні операції (ШсО) розглядаються як форма ведення психологічної боротьби та передбачають використання складної сукупності різних видів, способів і прийомів інформаційно-психологічного впливу, тобто впливу інформацією. ШсО починають проводиться в мирний час, активізуються в загрозливий період і повною мірою розгортаються у ході бойових дій.

ШсО в мирний час (загрозливий період) провадяться для досягнення наступних цілей:

- ізоляція ймовірного противника на міжнародній арені;
- підрив морально-психологічного стану військовослужбовців і населення противника;
- посилення антивоєнних і антиурядових настроїв у країні противника;
- консолідація населення й особового складу власних збройних сил і країн-союзників.

 Зміст ШсО в загрозливий період конкретизується в залежності від політичних і військових цілей конфлікту, військово-політичної обстановки на ТВД; розмаху діяльності опозиційних політичних партій, дисидентського та пацифістського рухів, а також особливостей психології, звичаїв, традицій і релігійних вірувань народу в країні противника.

У ході бойових дій ШсО переслідують наступні головні цілі:

- підрив морально-психологічного стану особового складу збройних сил противника;
- послаблення наступального пориву або здатності до завзятої оборони противника;
- деморалізація частин противника, що відходять, спонукання особового складу оточених (відсічених) підрозділів до здачі в полон.

Основними об'єктами ІПсО виступають:

1) військовослужбовці противника;
2) населення противника;
3) населення і військовослужбовці нейтральних і союзних держав.
4) військовослужбовці та населення своєї країни.

У межах психологічної боротьби сформувалася інформаційно-психологічна зброя. Під **інформаційно-психологічною зброєю** розуміють засоби і технології, які реалізують інформаційні впливи на психіку, в першу чергу, свідомість особи, соціальних груп, з метою впровадження необхідних ідеологічних і соціальних установок, формування помилкових стереотипів поводження та прийняття рішень, трансформації в потрібному напрямку їхніх настроїв, почуттів, волі.

На сьогодні, за механізмами реалізації фахівці виділяють **наступні види психофізичних впливів на психіку особи:**

1) пропагандистський,
2) нейролінгвістичний,
3) психоаналітичний,
4)психотронний,

5) психотропний,

6) психогенний.

Перші чотири з яких мають безпосередньо інформаційну ос нову.

*Пропагандистський **та** нейролінгвістичний впливи* на об'єкти (групи об'єктів) може здійснюватись:

■ друкованими засобами - шляхом підготовки і видання друкованої продукції (листівок, газет, буклетів і т.п.) на відповідній поліграфічній базі та її розповсюдження авіаційними, повітроплавальними, ракетно-артилерійськими, піротехнічними й іншими засобами, а також шляхом підготовки матеріалів і публікацій для поширення у засобах масової інформації;

• за допомогою електронних засобів - шляхом підготовки і передачі по теле- і радіоканалам, комп'ютерним мережам, телеграфним, телефонним, іншим лініям зв'язку, а також через штатні військові засоби спеціальних програм (передач), через входження у мережі бойового управління і канали зв'язку об'єктів (груп об'єктів) впливу через військові (корабельні) радіозасоби;

• безпосереднім (опосередкованим) спілкуванням - шляхом підготовки і передачі через штатні звукомовні засоби програм усного мовлення, а також організації мітингів, семінарів, проведення бесід, лекцій, доповідей і т.п., з використанням образотворчих засобів

• шляхом виготовлення спеціальних плакатів, транспарантів, наклейок, фотостендів, сувенірів з відповідною символікою і текстами на іноземних мовах, у перспективі - голографічних зображень тощо.

Психоаналітичний вплив здійснюється шляхом безпосереднього спілкування, а також за допомогою електронних засобів.

Новітнім видом інформаційно-психологічної зброї є ***психотронна зброя*** - спеціальні технічні засоби (психотронні генератори), які використовують вплив так званих енергоінформа-ційних полів. Окремо розглядають психотронні генератори,

психотронні формоутворюючі генератори, спінорні генератори, ретранслятори енергії космосу, багатополярні генератори.

Аналіз різновидів інформаційно-психологічної зброї свідчить як про надзвичайну небезпечність і різноманітність її видів, так і про небезпечність і різноманітність каналів її впливу - від засобів масової інформації до технологій та засобів впливу на свідомість і підсвідомість людей, що вкрай небезпечно у зв'язку з практичною відсутністю засобів контролю цих процесів. Приклади деяких способів інформаційно-психологічного впливу:

Голодування

Ефективний прийом емоційного впливу на електорат і психологічного тиску на владу. Підбирається група добре оплачуваних молодих людей з міцним здоров'ям, які нічим не ризикують, організовують «курс лікувального голодування» в публічному місці. Навкруги цього ЗМІ піднімають неймовірний галас. Постійно звучать звинувачення в жорстокості режиму, організації або конкретної особи. Проти цього прийому встояти дуже складно (за умови, що він проводиться професійного), оскільки влада у будь-якому випадку вимушена реагувати на вимоги, що висуваються «борцями».

Переписування історії

Метод ефективний в тривалій перспективі, коли вимагається поступово сформувати потрібний світогляд цілому суспільству, вчинити над ним програму маніпуляції і прибрати здоровий глузд декількох поколінь. Для цього треба в першу чергу зруйнувати історичну пам'ять.

Сучасні технології маніпуляції свідомістю здатні зруйнувати в людині знання, отримане від реального історичного досвіду, замінити його штучно сконструйованим знанням. Соціально-сформована картина історичної дійсності передається окремим індивідам за допомогою книг, лекцій, радіо і преси, театральних вистав, кінофільмів тощо.

Особливо ефективний кінематограф. Усі бачили американські бойовики «Рембо» і «Рембо - 2», тому знають, що Америка,

ганебно програвши війну у В'єтнамі, з успіхом виграла її на кіноекранах. Подібних фільмів Захід провів тисячі - і наповнив ними весь світ.

Ще однією популярною темою є переписування історії Другої світової війни. Подивившись американські блокбастери, ви, нарешті, зрозумієте, що хребет нацизму був зламаний не в Сталінграді та під Курськом, а під час порятунку з полону американського рядового Райана. А в суперфільмах «Сталінград» (1994) і «Ворог біля воріт» (2001) ви побачите, як шляхетні та цивілізовані німці мужньо б'ються проти російських дикунів і, загалом, виходять у Сталінграді переможцями. Причому німці, виявляється, були всі як на підбір антифашисти, «просто вони чесно виконували свій військовий обов'язок».

Успіхи західної пропаганди на цьому терені значні. Як зазначає у свій статті *В.Чмельов.* на питання, хто вперше створив атомну електростанцію, атомний криголам, штучний супутник Землі, наймогутнішу ракету-носій, кораблі на підводних крилах і повітряній подушці, вивів людину в космос, отримав вирішальну перемогу в Другій світовій війні, значна частина російської (!) молоді називає... Сполучені Штати Америки. Список таких псевдодосягнень Заходу можна продовжувати до безкінечності. В цей же час, деякі свої дійсні досягнення на Заході чомусь не афішують. Наприклад, пріоритет винаходу атомної бомби, а потім її випробування на мирних жителях Хіросіми та Нагасакі. (До речі, сьогодні ЗО % молодих японців щиро вважають, що ці міста і їх населення винищили росіяни, скинувши атомні бомби, а американці самовіддано рятували потерпілих).

Підміна змісту

Підміна - це один із варіантів горезвісних «подвійних стандартів». Полягає у використовуванні сприятливих визначень для позначення несприятливих дій (або навпаки). Основною метою застосування способу є створення сприятливого іміджу насильницьких дій. Так, погроми називаються «демонстрація-

ми протесту», бандитські формування - «борцями за свободу», найманці - добровольцями. Коли наші спецслужби ізолюють державних злочинців - це політичне репресії.

Психологічний шок

Сьогодні ЗМІ вводять видовище смерті в кожний будинок і у величезних кількостях. Ми постійно бачимо зображення убитих людей крупним планом - так, що їх не можуть не впізнати їх близькі. Ми дивимося на напівобгорілі трупи жертв катастроф і терактів. Це робиться для того, щоб під прикриттям шоку впровадити чисто політичні ідеї. Психологічний шок звичайно знімає всі психологічні захисти і пропагандистська абракадабра безперешкодно проникає в наш мозок. Так, дослідження показали, що відеоряд, що показує, наприклад, наслідки війни, має найсильнішу дію на підсвідомість і формує громадську думку проти сторони, що вчинила акт руйнування незалежно від того, чи є справедливою мета самої війни.

Але як інформаційна війна, так і інформаційне протиборство й інформаційна боротьба є проявами одного більш широкого поняття - загрози інформаційній безпеці. Саме це поняття і стане об'єктом нашого наступного розгляду.

4. Поняття загроз інформаційній безпеці

Аналізові змісту поняття «інформаційна безпека» зазвичай дослідниками приділяється значна увага, у той час як такі поняття, як небезпека і загроза розглядаються дещо спрощено і здебільшого у звуженому плані, відірваному від контексту поняття «інформаційна безпека».

Необхідність у розробленні поняття «загроза» визначається: 1) відсутністю єдиного підходу до дослідження основних понять інформаційної безпеки; 2) недостатньою розробленістю родового поняття «загроза» і питань його відмежування від інших споріднених понять, таких, як «небезпека», «виклик», «ризик», і відповідно видового «інформаційна загроза» і його відмежуван-

ня від таких понять, як «інформаційна війна», «інформаційне протиборство», «інформаційний тероризм»; 3) наявністю неви-рішеної проблеми формування категорійно-понятійного апарату теорії інформаційної безпеки; 4) можливістю на підставі теоретичних розробок даного апарату формувати адекватну систему моніторингу та управління загрозами та небезпеками в інформаційній сфері.

Найбільш широко загрози інформаційним ресурсам можна розглядати як потенційно можливі випадки природного, тех нічного або антропогенного характеру, які можуть спричинити небажаний вплив на інформаційну систему, а також на інформацію, яка зберігається в ній. Виникнення загрози, тобто відна ходження джерела актуалізації певних подій у загрози характеризується таким елементом, як уразливість. Саме за наявності вразливості як певної характеристики системи і відбувається активізація загроз. Безперечно, що самі загрози за своєю суттю відповідно до теорії множин є не вичерпними, а отже і не можуть бути піддані повному описові.

Інтегруючи різноманітні підходи, а також пропозиції щодо розв'язання даного питання™, вважаємо, що можна виділити такі ***види загроз інформаційній безпеці:*** розкриття інформаційних ресурсів; порушення їх цілісності; збій в роботі самого обладнання.

[86] *Зіма І.І,, Ніколаєв І.М. Інформаційна війна та інформаційна безпека (огляд думок зарубіжних політологів та воєнних спеціалістів) // Наука і оборона. -МІ.- 1998. - С. 56 - 58.; Рибак М.І., Атрохов А.В. До питання про інформаційні війни // Наука і оборона. - № 2. - 1998. -С. 65-68,; Лопатин В.Н. Информационная безопасность в системе государственного управления; Теоретические и организационно-право вые проблемы: Дис. ... канд. юрид. наук: 12.00.02. - СПб., 1997. - 193 с; Фатьянов АЛ. Правовое обеспечение безопасности информации: Дис... dpa юрид. наук: 12.00.02. - М., 1999. - 503 с.*

Розглянемо більш детально кожний з цих видів.

Загроза розкриття інформаційних ресурсів полягає у тому, що дані, інформація і знання стають відомими тим, кому не слід цього знати. У межах нашої роботи під *загрозою розкриття* розумітимемо такий стан, коли отриманий несанкціонований доступ до ресурсів системи, при чому йдеться як про відкриті, гак і і ті ресурси, які мають обмежений доступ. Ці ресурси мають передаватися один одному і зберігатися у єдиній інформаційній системі.

Загроза порушення цілісності інформаційних ресурсів полягає, в умисному антропогенному впливі (модифікація, видалення, зниження) даних, які зберігаються в інформаційній системі суб'єкта управління, а також передаються від даної інформаційної системи до інших.

Загроза збою в *роботі самого обладнання* може виникнути при блокуванні доступу до одного або декількох ресурсів інформаційної системи. Насправді блокування може бути постійним, так щоб ресурс, що запитується, ніколи не був отриманий, або може викликати затримання в отриманні ресурсу, що запитується, що є достатнім для того, щоб він став некорисним.

Відповідно до викладеного, розглянемо наступні загрози, які загрожують інформаційній безпеці. Розгляд даних загроз робиться з метою продемонструвати, що знання загроз і уразливих місць дозволить організувати адекватну систему управління інформаційною безпекою.

Найбільш частими та небезпечними є *ненавмисні помилки користувачів,* операторів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи. Іноді такі помилки є загрозами (невірно введені дані, помилка в програмі, котра викликає колапс системи), іноді вони створюють ситуації, якими не лише можуть скористатися зловмисники, а які самі по собі становлять безпосередню небезпеку об'єкта. Яскравим прикла-

дом є уведення невірної інформації в комп'ютер швейцарським оператором на землі, внаслідок чого у небі зіткнулося два літаки, в одному з яких летіли діти з Росії. Наслідки були трагічними як для пасажирів літака, так і для оператора, якого через деякий час після катастрофи було навмисно вбито.

У цілому ж, за результатами проведених фахівцями з інформаційної безпеки досліджень, понад 65 % шкоди, яка завдається інформаційним ресурсам, є наслідком ненавмисних помилок'[7]. Пожежі та землетруси, тобто загрози природного характеру, трапляються набагато рідше. Саме тому, доцільним є акцентування уваги на більшому впровадженні комп'ютерних систем для забезпечення безпеки. Плідною у даному контексті є пропонована програма Національним інститутом стратегічних досліджень «Електронна Україна»**.

Наступними, за розміром шкоди, можна виділити *крадіжки і підлоги.* У більшості випадків, суб'єктами вчинення даних дій були штатні працівники цих організацій, які є добре обізнаними у роботі інформаційної системи, а також заходів безпеки[4]".

У цьому аспекті дуже небезпечними є співробітники, які є незадоволеними або не поділяють цінностей тієї організації, де вони працюють. Одним з яскравих прикладів є дія колишнього генерала СБУ, одного з керівників ГУР України Валерія Кравченка, який 18 лютого 2004 року, маючи на руках матеріали з обмеженим доступом, безпідставно надав до них доступ іншим особам, зокрема журналістам Дойче Веле"".

У найбільш загальному плані діями ображених співробітників керує намагання нанести шкоду організації, в якій вони

[87] Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект. Фонд «Мир», 2003. - 640 с

[8Я] www.niss.gov.ua

"[9] Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект. Фонд «Мир». 2003. - 640 с.

"" www.korrespondent.net.

працювали, і яка, на їхню думку, їх образила. Така образа може знайти відображення у вчиненні наступних дій:

- пошкодження обладнання;
- вбудовування логічної бомби, яка з часом руйнує програми і дані;
- введення невірних даних;
- знищення даних;
- зміна даних;
- модифікація даних;
- надання доступу до даних із обмеженим доступом тощо.

Ображені співробітники обізнані з порядками в організації і здатні нашкодити вельми ефективно. Необхідно слідкувати за тим, щоб при звільненні співробітника його права доступу до інформаційних ресурсів були повністю обмежені, а після його звільнення змінені всі паролі доступу до внутрішньої мережі. Більш того, слід обмежити його спілкування із особами, які мають доступ до важливої інформації.

Окрім антропогенних, слід виділяти загрози *природного ха рактеру*. Загрози природного характеру характеризуються великим спектром. По-перше, можна виділити порушення інфраструктури: аварії електроживлення, тимчасово відсутній зв'язок, перебої із водопостачанням тощо. Небезпечними також є стихійні лиха, землетруси, урагани, смерчі, бурани, тайфуни тощо. Загальна процентна кількість інформаційних загроз природного характеру за даними американських аналітиків становить приблизно 14 відсотків від загальної кількосте".

Безперечно певну частку загроз становлять собою хакери, водночас їхня діяльність більше носить міфічний характер, а самі можливості хакерів є більше їхньою ж продукцією, яка лякає необізнаних. Насправді, щодня сервери органів державного управління підлягають атакам хакерів, водночас їхній загальний коефіцієнт шкоди порівняно зі шкодами іншого характеру вельми маленький.

"' *www.pccip.gov*.

Серйозною загрозою можуть бути *програмні віруси.* Водночас дотримання правил користування комп'ютерною технікою, а також наявність у штаті співробітників органу управління відповідного фахівця з даних питань значно полегшить розв'язання зазначених завдань.

Більш детально розглянемо класифікацію загроз. Отже, розкраданню підлягають:

■ апаратні засоби (блоки, вузли і готові вироби), якими осна щуються комп'ютери і мережі;

• носії програмного забезпечення та інформації;

■ тверді копії із роздрукованою інформацією.

Розкрадання може бути організовано з:

• робочих місць користувачів;

• у момент транспортування;

• з місць збереження.

Джерелами помилок у програмному забезпеченні (ПЗ) можуть бути:

• логічні помилки розробників програмного забезпечення;

• непередбачені ситуації, які проявляються при модернізації, заміні чи додаванні нових апаратних засобів, встановленні нових додатків, виході на нові режими роботи ПЗ, появі раніше не зафіксованих нештатних ситуацій;

• віруси, якими інфіковані програми;

• спеціальні програмні компоненти, які передбачені розробниками ПЗ для різного роду цілей.

Віруси самі по собі також становлять небезпеку і можуть знаходити свій вияв у видаванні повідомлень на екран монітора; затиранні інформації на дисках; переміщенні фалів до інших папок; уповільненні роботи комп'ютера; зборі інформації про роботу організації тощо.

Зважаючи на компетенцію органів державного управління, на наш погляд загрози атаки на їх інформаційні системи може здійснюватися з метою:

• встановлення доступу до інформації з обмеженим доступом;

• викрадення ключів, паролів, ідентифікаторів, списку користувачів;

ініціалізація контрольованого алгоритму роботи комп'ютерної системи;

• приведення у непридатність частини або всієї системи ор ганів державного управління.

Відповідно виділяють і види загроз. Через їх чисельність нами була зроблена спроба, з урахуванням існуючих напрацю-вань щодо питань класифікації загроз національній безпеці, виокремити загрози інформаційній безпеці"-.

За джерелами походження:

• *природного походження* - включають в себе небезпечні геологічні, метеорологічні, гідрологічні морські та прісноводні явища, деградацію ґрунтів чи надр, природні пожежі, масове ураження сільськогосподарських рослин і тварин хворобами чи шкідниками, зміна стану водних ресурсів і біосфери тощо;

• *техногеїіного походження* - транспортні аварії (катастрофи), пожежі, неспровоковані вибухи чи їх загроза, раптове руйнування каналів зв'язку, аварії на інженерних мережах і спорудах життєзабезпечення, аварії головних серверів органів державного управління тощо;

• *антропогенного походження* - вчинення людиною різноманітних дій з руйнування інформаційних систем, ресурсів, програмного забезпечення об'єкта тощо. До цієї групи за змістом дій належать: *ненавмисні,* викликані помилковими чи ненавмисними діями людини (це, наприклад, може бути помилковий запуск програми, ненавмисне інсталяція закладок тощо); *навмисні (інспіровані),* що стали результатом навмисних дій людей (наприклад: навмисне інсталяція програм, які передають інформацію на інші комп'ютери, навмисне введення вірусів тощо).

"[2] *Див. напр.: Ліпкан ВА. Теоретичні основи та елементи національної безпеки України: Монографія. - К.: Текст, 2003. - С. 333 - 343.*

За ступенем гіпотетичної шкоди:

• *загроза* - явні чи потенційні дії, які ускладнюють або унеможливлюють реалізацію національних інтересів в інформаційній сфері та створюють небезпеку для системи державного управління, життєзабезпечення її системостворюючих елементів;

• *небезпека* - безпосередня дестабілізація функціонування системи державного управління.

За повторюваністю **вчинення:**

• *повторювані* - такі загрози, які раніше вже мали місце;

• *продовжувані* - неодноразове здійснення загроз, що складається з ряду тотожних, які мають спільну мету.

За сферами походження:

• *екзогенні* - джерело дестабілізації системи лежить поза її межами;

• *ендогенні* - алгоритм дестабілізації системи перебуває у самій системі.

За ймовірністю реалізації:

• *імовірні* - такі загрози, які за виконання певного комплексу умов обов'язково відбудуться. Прикладом може слугувати оголошення атаки інформаційних ресурсів суб'єкта забезпечення національної безпеки, яке передує самій атаці;

• *неможливі* - такі загрози, які за виконання певного комплексу умов ніколи не відбудуться. Такі загрози зазвичай мають більше декларативний характер, не підкріплений реальною і, навіть, потенційною можливістю здійснити проголошені наміри, вони здебільшого мають залякуючий характер;

• *випадкові* - такі загрози, які за виконання певного комплексу умов кожного разу протікають по-різному. Загрози даного рівня доцільно аналізувати за допомогою методів дослідження операцій, зокрема теорії ймовірностей і теорії ігор, які вивчають закономірності у випадкових явищах.

За рівнем детермінізму:

■ *закономірні* — такі загрози, які носять стійкий, повторюваний характер, що зумовлені об'єктивними умовами існування

та розвитку системи інформаційної безпеки. Так, наприклад, будь-який суб'єкт ЗНБ буде піддаватись інформаційним атакам, якщо в ньому не функціонує, або функціонує не на належному рівні система забезпеченая інформаційної безпеки;

• *випадкові* — такі загрози, які можуть або трапитися, або не трапитися. До таких загроз належать загрози хакерів дестабілі зувати інформаційні системи суб'єктів ЗНБ, РНБОУ.

За значенням:

допустимі - такі загрози, які не можуть призвести до колапсу системи. Прикладом можуть слугувати віруси, які не пошкоджують програми шляхом їх знищення;

недопустимі - такі загрози, які: 1) можуть у разі їх реалізації призвести до колапсу і системної дестабілізації системи; 2) можуть призвести до змін, не сумісних із подальшим існуванням СНБ. Так, наприклад, вірус «i love you», спричинив пошкодження комп'ютерних систем у багатьох містах світу, і завдав загального збитку біля **100** мільйонів доларів США.

За структурою впливу:

• *системні* - загрози, що впливають одразу на всі складові елементи суб'єкта ЗНБ. Цей вплив має відбуватись одночасно в декількох найбільш уразливих і важливих місцях. Для суб'єкта ЗНБ це може бути цілеспрямована дискредитація їхніх праців ників через телебачення, радіомовлення, друковані засоби ма сової інформації, Інтернет. Яскравим прикладом була спроба системної дестабілізації у лютому 2003 року, коли Президент України Л. Кучма мав відвідати з офіційним візитом канцлера Німеччини Г.Шрьодера. Дещо нагадаємо події того часу. За тиж день до приїзду Президента України до міста, де мала відбутися зустріч посадовців прибуває майор Мельниченко і, як завжди, цочинає висвітлювати «нові факти», які розкривають «злочин ний правлячий режим Л. Кучми». Одночасно з цим генерал СБУ офіцер безпеки посольства України в Німеччині відмовляється повернутися на Батьківщину, більш того, починає також давати умовно відверті коментарі із демонстрацією документів з обме-

женим доступом німецькій радіохвилі. У цей же час в Інтернеті опозиційними силами також влаштовується нагнітання обстановки, яка дуже яскраво коментує події в Німеччині, при чому із такою обізнаністю і витонченістю, що все це видає дуже гарно сплановану виставу. Ці події відбуваються за межами України, у той час як всередині країни опозиція починає влаштовува ти також демонстративні акти, щоб привернути увагу світової спільноти до внутрішніх подій суверенної держави. Таким чином, спланована інформаційна провокація велася на системному рівні, тобто впливу були піддані життєво важливі елементи системи безпеки країни. Однак з урахуванням вже існуючих на-працювань, а також того факту, що українська влада усвідомила власну уразливість з боку інформаційних агресорів, були розроблені та впроваджені адекватні заходи нейтралізації і проведені відповідні інформаційні операції, які врешті-решт принесли позитивний результат, імідж нашої країни не було спаплюжено, а зустріч голів високих посадових осіб України та Німеччини відбулася у запланованих параметрах;

• *структурні* - загрози, що впливають на окремі структури системи. Дані загрози є також небезпечними, водночас вони стосуються структури окремих органів державної влади або їх компонентів. Так, наприклад, під час порушень процедури виборів мера м. Мукачево весною 2004 року була дискредитована як місцева влада, тобто нижня ланка системи державного управління, так і Міністерство внутрішніх справ України, тобто середня ланка і важливий суб'єкт забезпечення національної безпеки країни;

• *елементні* - загрози, що впливають на окремі елементи структури системи. Дані загрози носять постійний характер і можуть бути небезпечними лише за умови неефективності або непроведения їх моніторингу. Так, наприклад, свого часу, наприкінці 60 років XX століття, коли в Італії діяли так звані «Червоні бригади», влада не приділяла достатньо уваги діям терористів, які спочатку погрожували, а згодом почали фізично

ліквідовувати усіх суддів, які виносили звинувачувальні вироки терористам. Жертвою халатності та неадекватної оцінки інформаційної загрози став і тодішній прем'єр-міністр Італії Альдо Моро, якого було попереджено заздалегідь про напад, водночас влада не вжила відповідних заходів і його було викрадено, а згодом і вбито. Теж саме стосується подій із вчиненням актів тероризму 11 вересня 2001 року, про які американські спецслужби було попереджено заздалегідь, втім вони не сприйняли інформацію як достовірну.

За характером реалізації:

• *реальні* - активізація алгоритмів дестабілізації є неминучою і не обмежена часовим інтервалом і просторовою дією;

• *потенційні* - активізація алгоритмів дестабілізації можлива за певних умов середовища функціонування органу державного управління;

• *здійснені* - такі загрози, які втілені у життя;

• *уявні* - псевдоактивізація алгоритмів дестабілізації, або ж активізація таких алгоритмів, що за деякими ознаками схожі з алгоритмами дестабілізації, але такими не є.

За **ставленням** до **них:**

• *об'єктивні* - такі загрози, які підтверджуються сукупністю обставин і фактів, що об'єктивно характеризують навколишнє середовище. При цьому ставлення до них суб'єкта управління не відіграє вирішальної ролі через те, що об'єктивні загрози існують незалежно від волі та свідомості суб'єкта. Так, прикладом, хоча український законодавець у Законі України «Про основи національної безпеки України» не визначив пріоритетність захисту від інформаційних загроз, відвівши їм найменшу увагу, насправді їх значення є непересічним, і акцентування уваги на інших загрозах призводить постійно до разючих помилок в сфері саме інформаційній;

• *суб'єктивні* - така сукупність чинників об'єктивної дійсності, яка вважається суб'єктом управління системою безпеки загрозою. За даного випадку визначальну роль у ідентифікації

тих чи інших обставин та чинників відіграє воля суб'єкта управління, який і приймає безпосереднє рішення про надання статусу або ідентифікації тих чи інших подій в якості загроз безпеці. За об'єктом впливу:

- На державу; ■

На людину;

- На суспільство.

За формами закріплення:

нормативні - офіційно усвідомлені і визнані як такі в нормативних актах країни. В Україні, наприклад, дані загрози визначені в Законі України «Про основи національної безпеки України», в Росії - у «Доктрині інформаційної безпеки»;

ненормативні - існують об'єктивно, але не є усвідомленими вищим політичним керівництвом держави і не знайшли адекватного віддзеркалення у нормативній системі держави.

У даній класифікації ми намагалися продемонструвати багатоманітність і неоднаковість, багатошаровість і певну нескінченість загроз та небезпек інформаційній безпеці, які є адекватними часу і простору, темпам розвитку суспільства.

Висновки

Отже, за інтенсивністю, масштабами та засобами, які використовуються, виділяють:

інформаційна експансія - діяльність для досягнення національних інтересів методом безконфліктного проникнення в інформаційну сферу;

інформаційна агресія ~ незаконні дії однієї зі сторін в інформаційній сфері, спрямовані на нанесення супротивнику конкретного відчутного збитку в окремих областях його діяльності шляхом обмеженого і локального по своїх масштабах застосування сили;

інформаційна війна — найвищий ступінь інформаційного протиборства, спрямований на розв'язання суспільно-політич-

 них, ідеологічних, а також національних, територіальних та інших конфліктів між державами, народами, націями, класами й соціальними групами шляхом широкомасштабної реалізації засобів і методів інформаційного насильства (інформаційної зброї). У концептуальному плані потребують вирішення наступні проблеми.

1. Реорганізація системи інформаційної безпеки держави. Як основні компоненти вона повинна включати: структури, націлені на ведення інформаційного протиборства зі створення умов для реалізації національних інтересів; координуючий орган, підпорядкований безпосередньо Президенту України. Причому підсистеми інформаційної боротьби, створені у кожного з суб'єктів забезпечення національної безпеки, мають бути функціонально включені до загальної системи інформаційної боротьби, котра у свою чергу, входитиме до системи забезпечення інформаційної безпеки.

2. Розроблення концепції ведення інформаційного протиборства як на міжнародному, державному і регіональному рівнях, так і на рівні окремих суб'єктів забезпечення інформаційної безпеки.

3. Вироблення механізмів взаємодії і координації між суб'єктами системи забезпечення інформаційної безпеки.

4. Розроблення методики виявлення на початковому етапі ознак ведення інформаційно-психологічних операцій проти держави в цілому, і проти суб'єктів ЗНБ - зокрема.

5. Розроблення нормативно-правової бази у сфері контролю за інформаційним простором держави в мирний час та передачі цих повноважень Генеральному штабу ЗС України на особливий період.

6. Заборона на міжнародному рівні виробництва і застосування засобів інформаційно-енергетичного впливу на людину (психотронної зброї) і розробка заходів та засобів захисту від неї.

Проблема забезпечення інформаційної безпеки на сучасному етапі є однією з ключових у процесі забезпечення національної

безпеки будь якої сучасної держави, зокрема, України. Вона повинна розглядатись на базі єдиних методологічних підходів, вироблених в межах націобезпекознавства.

Іінформаційна боротьба поступово стане самостійним видом військових дій. Інформаційна зброя стане системоруинуючою тобто зможе виводити з ладу цілі бойові, економічні і соціальні системи. Очікується також поява «інтелектуальної» інформаційної зброї, нових її зразків на базі нано- та біотехнологій. Передбачається поява одного з найбільш небезпечних видів інформаційної зброї нелетальної дії - психотронної зброї. Таким чином, три традиційні сфери ведення бойових дій: суша, море, повітря, поповняться новою четвертою сферою - інформаційною, в якій діятимуть сили інформаційної боротьби.

Розвиток інформаційної зброї призведе до того, що в майбутньому виникнуть інформаційні війни, які будуть вестись в інформаційному просторі в основному інформаційними засобами і забезпечувати досягнення стратегічних політичних, економічних та інших цілей.

Інформаційні війни стануть реальністю, ігнорування якої уже **в** наш час є недопустимим. Відтак країни, які не матимуть розробленої концепції національної безпеки, і відповідно, доктрини інформаційної безпеки, а в її рамках стратегії інформаційної боротьби, ризикують залишитися на узбіччі світової цивілізації. Така перспектива загрожує новим поділом країн світу за ознакою рівня розвитку інформаційної сфери.

Ключові терміни та поняття

Інформаційна війна, інформаційне протиборство, інформаційна зброя, інформаційна боротьба, інформаційна агресія, інформаційна експансія, інформаційна перевага

Контрольні запитання для самоперевірки

1. Дайте визначення поняттям «загроза», «небезпека».

2. Назвіть основні характеристики загроз інформаційній безпеці України.

3. Як співвідносяться категорії «небезпека» та «загроза»?

4. Які існують основні підходи виокремлення безпекогенних чинників?

5. Визначте види загроз за певними критеріями.

6. Назвіть базові загрози інформаційній безпеці держави.

7. Назвіть базові загрози інформаційній безпеці суспільству.

8. Назвіть базові загрози інформаційній безпеці людині, громадянину.

Завдання для самопідготовки

1. Яким чином загроза національним інтересам впливає на національну безпеку?

2. Окресліть ієрархію безпекогенних чинників у інформаційній сфері

Список рекомендованої літератури

Нормативні джерела

1. *Конституція* України // Відомості Верховної Ради (ВВР). -1996.-№30. -Ст. 141.

2. Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. // Российская газета. - 2000. - 28 сентября.

Доктринальні джерела

1. *Волковскии Н.Л.* История информационных воен. В 2 ч. 4.2 /СПб.: ООО «Издательство Полигон», 2003. -756с.

2. *ГольевА.* Служба психологических операций Войска Польского. */І* Зарубежное военное обозрение.— 2005. -№3. С.45-52.

3. *Гриняев С.* Взгляды военных экспертов США на ведение информационного противоборства // Зарубежное военное обозрение. - 2001. - № 8. С.10-12.

4. *Гриняев С.* Концепция ведения информационной войны в некоторых странах мира // Зарубежное военное обозрение. -2002. -№2.С. 11-15.

5. *Гриньов С. В.* Война в четвертой сфере: Превосходство в киберпространстве будет определять победу в конфликтах XXI века // Независимое воен. обозрение. - 2000. - №3. - С. 7-8.

6. *Жук СЯ.* Інформаційне протиборство: стан і проблеми// Матеріали круглого столу «Актуальні проблеми забезпечення національної безпеки України» (Київ. Нац. Ун-т внутр. Справ, 06 грудня 2005 року). - К.: Текст, 2006.

7. *Зіма І. І., Ніколаєв І. М.* Інформаційна війна та інформаційна безпека (огляд думок зарубіжних політологів та воєнних спеціалістів) // Наука і оборона. - № 1. - 1998. - С. 56-58.

8. *Кара Мурза* С. *Г.* Манипуляция сознанием. - К.: Діалектика, 2000. - 448 с.

9. *Кормич Б А.* Організаційно-правові засади політики інформаційної безпеки України: Монографія.- Одеса: Юридична література, 2003.- 472 с

10. *Лигпвиненко О.В.* Спеціальні інформаційні операції. / Рада національної безпеки і оборони України; Національний ін-т стратегічних досліджень. - К: НУСД, 1999. - 163 с

11. *Ліпкан ВА.* Безпекознавство: Навч. посібник.-К.: Вид-во Європ. ун-ту, 2003. - 208 с.

12. *Ліпкан ВА.* Інформаційна безпека як складова національної безпеки України // Інформаційні технології в економіці, менеджменті і бізнесі: Проблеми науки, практики і освіти: 36. наук, праць VIII Міжнар. наук.-практ. конф.— Ч. 2. — К.: Вид-во Європ. ун-ту, 2003. - с. 443 - 453.

13. *Ліпкан ВА.* Теоретичні основи та елементи національної безпеки України: Монографія.- К.: «Текст», 2003.- 600 с

14. *Лопатин В.Н.* Информационная безопасность России: Человек. Общество. Государство./Санкт-Петербургский университет МВД России.- СПб.:Фонд «Университет», 2000.- 428 с.

15. *Монойло А.В., Петренко А.И., Фролов О.Б.* Государственная информационная политика в условиях информационно-психологической войны.- М.: Горячая линия. Телеком, 2003. -541с.

16. *Почепцов Г.Г.* Информационные войны.-М.: «Руфл-бук»,К.: «Ваклер».-2001.-576 с.

17. Рибак М. І., Атрохов А. В. До питання про інформаційні війни /*І* Наука і оборона. - № 2.- 1998. - С. 65-68.

18. *Рибак М.І., Атрохов А.В.* До питання про інформаційні війни *И* Наука і оборона. - 1998. - № 2 - С. 65-68.

19. *Стеценко Ю.В.* Засоби масової інформації - відкриті носії прихованих повідомлень членів організованих злочинних груп і терористичних організацій // Актуальні проблеми політики: Зб.наук.праць / Голов.ред. С.В. Ківалов; відп. за вип. В.М. Дрьо-мін.- Одеса: Фенікс, 2004.- Вип.21.- С.237.

20. *Толубко В.Б., Жук С.Я., Косеецов В.О.* Концептуальні основи інформаційної безпеки України // Наука і оборона.-2004. -№2. С 19-25.

21. *Чмельов В.О.* Форми і засоби ведення інформаційної боротьби // Матеріали круглого столу «Актуальні проблеми забезпечення національної безпеки України» (Київ. Нац. Ун-т внутр. Справ, 06 грудня 2005 року). - К.: Текст, 2006 - с.

22. *ШвецД.Ю.* Информационная безопасность России и современные международные отношения.- М.: «Мир безопасности», 2001.-176с.

РОЗДІЛ 4
ДЕРЖАВНА ПОЛІТИКА НАЦІОНАЛЬНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Вступ

Окреслення державної політики національної безпеки є наступним важливим моментом інформаційної безпекової політики держави, оскільки саме від основних напрямів цієї політики залежатиме структура суб'єктів забезпечення інформаційної безпеки, а не навпаки. Структура є похідною від тих завдань, які ставить перед собою держава в інформаційній сфері, у свою ж чергу, інформаційна політика слугує своєрідним синтезом прагнень держави, її можливостей щодо реалізації цих прагнень і загроз національній безпеці в інформаційній сфері. Відтак, відповідно до націобезпекознавчого підходу, державна інформаційна політика є визначальною для формування системи забезпечення інформаційної безпеки, а остання є похідною від неї. Саме це зумовлює розгляд нами загальних теоретичних підвалин формування державної інформаційної політики.

1. Поняття державно-правового механізму інформаційної безпеки

Поняття «політика» здебільшого є політологічною категорією, під якою розуміють організаційну, регулятивну й контрольну сферу суспільства, в межах якої здійснюється соціальна діяльність, спрямована головним чином на досягнення, утримання й реалізацію влади індивідами й соціальними групами задля ствердження власних значущих інтересів і потреб.

Як зазначають *В.П. Горбатенко, Г.О. Лебединська,* нині існує широке коло наукових тлумачень, з яких політика постає як: одна зі сфер життєдіяльності суспільства; система певних суспільних відносин, взаємодія класів, націй, держав між собою і

владою; сукупність дій, заходів, установ, за допомогою яких узгоджуються інтереси різних верств населення тощо.

Політика держави та інформація - це взаємопов'язані явища, що перебувають в діалектичному взаємозв'язку в процесі функціонування державно-правових інституцій.

Слушною є думка *Арістової І.В.,* яка зазначила, що «якість інформації та її доступність, сучасні інформаційні технології, що радикально збільшують обсяг і швидкість поширення інформації, викликають глибокі зміни в політиці конкретної держави, чинять суттєвий вплив на характер і системи владарювання (точна інформація підвищує ефективність влади, дозволяє вчасно скоригувати обраний напрямок дій, відреагувати на обставини, що знову з'явилися). Водночас і політичні структури впливають на інформацію, ступінь її відкритості, процеси доставки, характер передачі споживачу. Одна з найважливіших соціальних функцій влади - дозування інформації та її «пакування». На цьому засновується механізм маніпулювання громадською думкою. Наивідомішою і простою формою владного контролю над інформаційними процесами виступає цензура, коли держава за допомогою спеціально призначених та відповідальних перед ним чиновників «керує» змістом друкарських та інших інформаційних матеріалів».

Одним зі способів регулювання вищезгаданого зв'язку служить право як система загальнообов'язкових, гарантованих державних норм, що виражають волю держави та виступають регулятором суспільних відносин.

Основною метою державної влади в період глобальної інформаційної революції є розробка та реалізація концептуальних основ державної інформаційної політики шляхом прийняття адекватних нормативно-правових актів щодо регулювання інформаційних відносин.

Кормич БА. зазначає, що забезпечення інформаційної безпеки повинно здійснюватись передусім, шляхом проведення вива-

женої і збалансованої політики держави в інформаційній сфері, яка має три основні вектори:

1) захист інформаційних прав та свобод людини;
2) захист державної безпеки в інформаційній сфері;
3) захист національного інформаційного ринку, економічних інтересів держави в інформаційній сфері, національних виробників інформаційної продукції.

Як засвідчує досвід провідних країн світу, великого значення для нормального функціонування інформаційної сфери держави набуває узгоджена діяльність відповідного державно-правового механізму, тобто система взаємопов'язаних державних органів, організацій, установ щодо вироблення та реалізації сукупності норм та принципів права, які повинні врегулювати суспільні відносини в інформаційній сфері.

Отже, в свою чергу, під *державно-правовим механізмом інформаційної безпеки* слід розуміти систему взаємопов'язаних й взаємоузгоджених державно-правових інституцій, завданнями яких є створення умов для успішної реалізації інформаційної політики.

Як зазначає *Кормич БА.,* ефективність захисту інформаційної безпеки держави в цілому забезпечується ефективністю кожної складової її державно-правового механізму, який складається з трьох взаємопов'язаних елементів.

По-перше, це сукупність державних інституцій, задіяних у процесі формування і впровадження політики інформаційної безпеки, тобто інституціональний механізм інформаційної безпеки.

По-друге, це сукупність ролей та відносин, яка включає правові відносини, що виникають при проведенні політики інформаційної безпеки та специфічні ролі. Форми і методи діяльності суб'єктів проведення цієї політики.

По-третє, це ієрархічна сукупність правових норм та принципів, яка регулює зміст та процес проведення політики інфор-

 маційної безпеки, тобто правовий механізм інформаційної безпеки.

Необхідно зазначити, що на початку 90-х років політика української держави в інформаційній сфері була здебільшого спрямована на створення техніко-технологічної інфраструктури. Починаючи з середини 90-х років, головною особливістю інформаційної політики нашої країни стає декларація про розроблення засад щодо реалізації інформаційних прав і свобод людини **і** громадянина. Отже, протягом десяти років здійснилась зміна пріоритетів у гаслах, від політики інформатизації до інформаційної політики держави. Утім на практиці від поставлення та вироблення цілей до їх конкретної реалізації та отримання шуканого результату ще далеко.

2. Поняття та особливості інформаційної політики держави

Під ***інформаційною політикою держави*** розуміють діяльність держави в інформаційній сфері, спрямованої на задоволення інформаційних потреб людини і громадянина через формування відкритого інформаційного суспільства на основі розвитку єдиного інформаційного простору цілісної держави та його інтеграції у світовий інформаційний простір з урахуванням національних особливостей **і** інтересів при забезпеченні інформаційної безпеки на внутрішньодержавному та міжнародному рівнях.

Основною метою політики інформаційної безпеки держави є управління реальними та потенційними загрозами та небезпеками з метою створення необхідних умов для задоволення інформаційних потреб людини та громадянина, а також реалізації національних інтересів.

Відтак, *державна політика інформаційної безпеки України* - діяльність державно-правових інституцій щодо управління реальними та потенційними загрозами та небезпеками з метою

задоволення інформаційних потреб людини та громадянина, а також реалізації національних інтересів.

Таким чином, *інформаційна політика України* та *держав-на політика інформаційної безпека* співвідносяться як ціле та частина, а тому дещо проаналізуємо особливості інформаційної політики в Україні.

Слушними є пропозиції *Арістової І.В.,* яка зазначила, що для реалізації національних інтересів в інформаційній сфері слід переглянути пріоритети державної політики, розробити нові концептуальні підходи щодо регулювання ринку інформаційно-комунікаційних технологій, інформаційної та інвестиційної політики, розвитку інформаційного законодавства і забезпечення інформаційної безпеки. Для вирішення даного завдання доцільно зважати на наступні моменти.

1. Створення умов для зростання інформаційної індустрії - під тримка розвитку комплексу галузей, які виробляють різноманітні інформаційні продукти та надають послуги в інформаційній сфері шляхом залучення інвестицій приватного сектору, створення зба лансованого конкурентного середовища і розвитку інформаційної інфраструктури українського ринку інформаційно-комунікацій них технологій.

2. Покращення доступу населення до інформаційної інфраструктури та мережевих послуг шляхом розвитку бібліотечної мережі, покращення довідково-інформаційного обслуговування населення та створення відповідних соціально сприятливих умов для використання інформаційно-комп'ютерних технологій (ІКТ).

3. Створення умов для розвитку базових навичок щодо використання можливостей, які надаються інформаційним суспільством, через забезпечення використання мережевих технологій у бібліотеках, вузах, школах, сприяння підвищенню комп'ютерної грамотності населення, його поінформованості щодо можливостей та ресурсів Інтернета, засвоєння переваг інформаційного обміну у всіх сферах діяльності людини та суспільства.

4. Підтримка наукових досліджень та соціально значущих застосувань ІКТ шляхом підтримки перспективних вітчизня них досліджень та розробок в галузі ІКТ, стимулювання іннова ційних застосувань ІКТ у всі сфери життя, покращення доступу до ризикового фінансування, реформування структури науко вих організацій і формування дослідницьких центрів світового класу.

5. Розвиток інформаційно-телекомунікаційних систем та формування інформаційних ресурсів в інтересах державного уп равління шляхом покращення доступу до державної інформації, удосконалення процедур надання послуг, підтримки державних інформаційних центрів, розвитку електронної взаємодії між органами державної влади на центральному, регіональному, місцевому рівнях і створення інтегрованої, орієнтованої на ко ристувача, системи державних інформаційних послуг на основі інформаційно-телекомунікаційної системи державних струк тур, тобто забезпечення доступності комп'ютерної інформації через комп'ютерні мережі, створення загальнодоступних сайтів та підключення до мережі відкритих суспільно-значущих де ржавних інформаційних ресурсів.

3. Напрями державної інформаційної політики

Відповідно до вищевикладеного, виокремлюють напрями державної інформаційної політики. До основних з них належать.

1. Удосконалення законодавства та правового регулювання у інформаційній сфері (в галузі створення та використання інформаційних ресурсів та технологій, реалізації інформаційних прав громадян і прав на результати творчої праці (інтелектуальна власність), регулювання функціонування українських сегментів глобальних інформаційних мереж (Інтернет), охорони прав користувачів інформаційних послуг та продуктів, захист молодого покоління від шкідливого впливу певних видів інформації та послуг, визначення балансу між потребою у вільному

обміні інформацією та припустимими обмеженнями на її поширення, регулювання питань захисту державної та комерційної таємниці).

2. Забезпечення інформаційної безпеки та захисту інформації (розвиток нормативного регулювання в галузі захисту даних у телекомунікаційних мережах; покращення та поширення про цедур надійної ідентифікації та аутентифікації; стимулюван ня використання надійних систем криптографії операторами мереж, особливо на ризикованих ділянках (супутниковий або мобільний зв'язок); використання стандартів безпеки для клю чових або громадських функцій, у тому числі введення (там, де це необхідно) обов'язкового контролю якості інформаційних процесів; розробка превентивних технічних засобів для забезпе чення надійності телекомунікацій; розробка мінімальних стан дартів безпеки для операторів та постачальників телекомуніка ційних послуг).

3. Розширення міжнародного співробітництва та торгівлі в галузі ІКТ (гармонізація українського законодавства з міжна родним, забезпечення взаємодії українських інформаційних систем із зарубіжними аналогами, створення сприятливих умов для формування єдиного інноваційного та інформаційного про стору між країнами СНД на базі загального ринку інформації, товарів, послуг, капіталів та робочої сили).

Одразу ж зазначимо, що підходи до формування напрямів державної політики інформаційної безпеки мають декілька векторів. Так, дані підходи можна окреслювати з огляду на необхідність досягнення певно визначеної мети, наприклад формування інформаційного суспільства. З іншого боку, дані напрями можуть корелювати із загрозами національній безпеці та національним інтересам в інформаційній сфері. Даний підхід репрезентовано у Законі України «Про основи національної безпеки і оборони України».

У ст. 8 даного закону визначені такі основні напрями державної політики національної безпеки в інформаційній сфері:

- забезпечення інформаційного суверенітету України;
- вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;
- активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України;
- забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступ до інформації, недопу щення неправомірного втручання органів державної влади, ор ганів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері та переслідування журналістів за політичні позиції;
- вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформацій ної сфери України.

4. Нормативно-правова основа політики національної безпеки в інформаційній сфері

Зазначимо, що в Україні вже розроблено проект *Концепції* ***національної інформаційної політики,*** в якому визначені правові, економічні та організаційні засади національної інформаційної політики та інформаційної безпеки держави. Розглянувши даний Проект, Верховна Рада України доручила Комітету з питань свободи слова та інформації його доопрацювати та внести його на розгляд у другому читанні.

За основу даної Концепції взято ряд важливих та цікавих для розгляду указів Президента України.

Так, на підставі Указу Президента України від 21 червня 1997 року «Про рішення Ради національної безпеки і оборони України

«Про невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин» від 17 червня 1997 року» Кабінету Міністрів України, Службі безпеки України та Міністерству оборони, Міністерству зв'язку України, Міністерству інформації Україні, Міністерству закордонних справ України та іншим міністерствам, Національній раді України з питань телебачення і радіомовлення були покладені ряд завдань, виконання яких сприятиме розвитку інформаційної політики в сфері забезпечення інформаційної безпеки, а саме: *1. Кабінету Міністрів України:*

- подати пропозиції щодо реформування системи державного управління;
- розробити та запровадити план заходів щодо реформування інформаційно-аналітичної системи органів державної влади;
- розробити концепцію розвитку і використання інформаційного простору України;
- внести пропозиції щодо створення єдиної системи формування, використання і захисту національних інформаційних ресурсів та інформаційного простору;
- розробити та затвердити державну програму здійснення інформаційної політики та розвитку національного інформаційного простору з урахуванням наявного соціально-економічного, науково-технічного і промислово-виробничого потенціалу держави, її матеріально-технічних, трудових, інформаційних ресурсів;
- вжити заходів до вдосконалення державної реєстрації суб'єктів інформаційної діяльності;
- підготувати пропозиції про внесення змін до законодавства України щодо встановлення відповідальності посадових осіб за протизаконне обмеження конституційного права на свободу слова або дії, спрямовані на поширення інформації, що не базується на достовірних даних, обмежує права громадян, завдає шкоди їх репутації чи державним інтересам України;

- вивчити питання про відповідність тарифів на розповсюдження друкованих періодичних видань реальній вартості цих послуг і в разі можливості здійснити заходи щодо їх здешевлення та підвищення конкурентоспроможності вітчизняних газет та журналів;

- проаналізувати прибутковість засобів масової інформації загальнодержавної сфери розповсюдження, підготувати та внести пропозиції щодо сприяння підвищенню ефективності їх економічної діяльності, забезпеченню реальної незалежності, в тому числі від тіньового капіталу;

- забезпечити систематичне вивчення рівня популярності серед населення друкованих видань, заснованих за участю державних органів, і вжити невідкладних заходів щодо підвищення впливовості цих видань на формування громадської думки;

- розглянути питання про надання цільової підтримки державним книжковим видавництвам;

- вжити невідкладних заходів для вирішення проблем, пов'язаних з функціонуванням бібліотек усіх рівнів;

- розробити і затвердити план заходів щодо забезпечення скоординованої діяльності у сфері виготовлення і розповсюдження інформаційних та рекламних матеріалів про Україну, її економічний потенціал, науку і культуру;

- проаналізувати рівень захисту державних інформаційних ресурсів та інформаційного середовища, систем зв'язку і теле-комунікацій, комп'ютерних інформаційних систем та здійснити необхідні заходи для створення національної інфраструктури інформаційної безпеки;

- визначити головну організацію, яка матиме право контролювати стан захисту державної таємниці в центральних органах державної влади, установах, на підприємствах, що виконують роботи, пов'язані з державною таємницею, або зберігають її носії;

2. Службі безпеки України та Міністерству оборони України подати пропозиції щодо порядку здійснення криптографічних заходів охорони державної таємниці.

3. Міністерству інформації України, Національній раді України з питань телебачення і радіомовлення разом з Міністерс твом закордонних справ України підготувати план заходів щодо забезпечення необхідної присутності України у світовому інформаційному просторі, насамперед, шляхом розвитку за кордоном мережі державних кореспондентських пунктів і створення державного супутникового каналу мовлення з визначенням джерел фінансування цієї діяльності.

4. Міністерству інформації України разом з Міністерством зовнішніх економічних зв'язків і торгівлі України, Міністерством закордонних справ України, Міністерством України у справах науки і технологій, Національним агентством України з реконструкції та розвитку, іншими центральними органами виконавчої влади розробити спільний план дій щодо забезпечення державної підтримки національних теле- і радіовиробників, друкованих засобів масової інформації.

5. Національній раді України з питань телебачення і радіо мовлення та Міністерству фінансів України розробити та подати пропозиції щодо розповсюдження реклами товарів (робіт, послуг) вітчизняного виробництва по ефірним і кабельним каналам мовлення на пільгових умовах.

6. Національній раді України з питань телебачення і радіомовлення, Міністерству інформації України, Міністерству зв'язку України, Головному управлінню з питань радіочастот при Кабінеті міністрів України, Міністерству внутрішніх справ України разом з Генеральною прокуратурою України вжити невідкладних заходів до припинення діяльності суб'єктів інформаційної діяльності, які порушують Конституцію України та закони України.

Наступним нормативно-правовим актом, що регулює суспільні відносини в сфері інформаційної політики став Указ Президента України від 6 грудня 2001 року ***«Про*** *рішення* ***Ради національної безпеки і оборони України «Про заходи щодо вдосконалення державної інформаційної політики та***

забезпечення інформаційної політики» від 31 жовтня 2001 року».

Згідно з цим Указом був визнаний незадовільним стан виконання Кабінетом Міністрів України, Державним комітетом інформаційної політики, телебачення і радіомовлення України, Державним комітетом зв'язку та інформатизації України Указів Президента України від 21 липня 1997 року «Про рішення Ради національної безпеки і оборони України від 17 червня 1997 року «Про невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин», від 14 липня 2000 року «Про вдосконалення інформаційно-аналітичного забезпечення Президента України та органів державної влади», від 31 липня 2000 року «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» та ряду інших нормативно-правових актів.

Внаслідок чого, Кабінету Міністрів України доручили провести службове розслідування причин невиконання зазначених нормативно-правових актів і доручень Президента України та вжити заходів щодо притягнення до відповідальності винних у цьому осіб, а також з метою удосконалення інформаційної політики та забезпечення інформаційної безпеки були поставлені наступні завдання:

1. Подати на розгляд Верховної Ради України проект Концепції національної інформаційної політики та інформаційної безпеки України, проект Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», розробити пропозиції щодо кодифікації законодавства в галузі інформаційних відносин та проект Стратегії впровадження національної інформаційної політики, а також розробити проект Національної програми розвитку вітчизняної теле- та радіоіндустрії з урахуванням довгострокових потреб розвитку телекомунікаційних мереж, засобів зв'язку, національного сегмента мережі Інтернет,

супутникових систем передачі інформації, супутникового та кабельного телебачення та вирішити в установленому порядку питання про її затвердження;

2. Розробити заходи щодо оптимізації системи державних органів, які реалізують інформаційну політику, забезпечивши чітке розмежування повноважень і налагодження їх взаємодії та координації, створення організаційної структури системи забезпечення інформаційної безпеки;

3. Проаналізувати виконання Національної програми інформатизації, переглянути проекти програм в інформаційній сфері, які фінансуються з Державного бюджету України, вжити заходів щодо першочергової реалізації та повноцінного фінансування найактуальніших із них;

4. Подати пропозиції щодо розвитку кабельного телебачення і проводового мовлення в регіонах України, створення Центру безпеки українського сегмента мережі Інтернет і Центру анти-вірусного захисту інформації;

5. Підготувати законопроект про внесення змін до законодавства, передбачивши в ньому ліцензування діяльності провайдерів на території України щодо надання доступу до мережі Інтернет;

6. Подати пропозиції стосовно створення системи стандартів щодо захисту інформації про озброєння, військову техніку та військово-промислові об'єкти та організаційно-методичного забезпечення системи захисту інформації у сферах взаємодії управлінь Озброєння Міністерства оборони України з оборонно-промисловим комплексом;

7. Вжити заходів щодо реалізації Положення про державне замовлення на створення і розповсюдження теле- та радіопрограм з урахуванням нагальної потреби підвищення якості інформаційної продукції;

8. Подати на розгляд Верховної Ради України законопроекти про внесення змін до законодавства, що регулює питання боротьби з комп'ютерною злочинністю, та про створення відповідного міжвідомчого центру;

9. Вивчити питання стосовно права іноземців і осіб без гро мадянства на заснування друкованого засобу масової інфор мації, одержання фізичними особами свідоцтва про держав ну реєстрацію періодичного друкованого видання лише в разі створення ними редакції як юридичної особи та заборони за снування і діяльності засобів масової інформації, у статутно му фонді яких більш як ЗО відсотків іноземних інвестицій, та в разі необхідності подати на розгляд Верховної Ради України пропозиції про внесення відповідних змін до законодавства України;

10. Опрацювати заходи щодо дальшого розвитку національного інформаційного ринку на конкурентних засадах, створення сприятливого інвестиційного клімату для розвитку вітчизняних засобів масової інформації та книговидання;

11. Розробити пропозиції щодо створення захищеної інформаційно-телекомунікаційної системи органів державної влади, яка б надавала телекомунікаційні послуги, передбачивши заходи щодо прискорення розробки вітчизняних засобів криптографічного та технічного захисту інформації;

12. Затвердити Програму створення та розгортання вітчизняного виробництва засобів захисту інформації, національної захищеної інформаційної системи, захищених систем електронного документообігу та електронного цифрового підпису, сертифікації технічних і програмних засобів інформатизації на відповідність вимогам інформаційної безпеки;

13. Розробити Єдину систему класифікації та кодифікації продукції оборонного та подвійного призначення, що експортується Україною;

14. Визначити механізм реалізації повноважень Генерального штабу Збройних сил України щодо участі в організації і контролі за інформаційним простором держави та його здійснення в особливий період;

15. Створити міжвідомчу робочу групу з представників заін-тересованих міністерств та інших центральних органів виконав-

чої влади для розроблення Національної геоінформаційної системи.

Даним Указом також покладені досить серйозні завдання й на інші державні інституції, а саме:

1. Проведення Антимонопольним комітетом України перевір ки додержання регіональними телерадіоорганізаціями антимо нопольного законодавства України;

2. Опрацювання заходів щодо запобігання контрабандному ввезенню на територію України видавничої продукції та її незаконному розповсюдженню Державною митною службою України, Державним комітетом у справах охорони державного кордону України та Міністерством внутрішніх справ України;

3. Вжиття заходів щодо розвитку зовнішньої інформаційної діяльності, інформування світової громадськості про Україну з метою формування позитивного її сприйняття у світі, щодо організації та фінансування теле- і радіомовлення за кордон Міністерством закордонних справ України, Державним комітетом зв'язку та інформатизації України, Державним комітетом інформаційної політики, телебачення і радіомовлення України;

4. Вдосконалення роботи з протидії інформаційним агресіям та спеціальним інформаційно-пропагандистським операціям, здійснюваним проти України іноземними спецслужбами Службою безпеки України;

5. Опрацювання Міністерством освіти і науки України разом з Департаментом спеціальних телекомунікаційних систем і захисту інформації Служби безпеки України заходів щодо підготовки та перепідготовки спеціалістів у сфері інформаційної безпеки; підготувати типові навчальні програми для середніх і вищих навчальних закладів з навчальної дисципліни «Інформаційна культура»; опрацювання разом з Міністерством економіки та з питань європейської інтеграції України, Державним комітетом інформаційної політики, телебачення і радіомовлення України, Українською Академією державного управління при Президентові України, Київським національним університетом

 ім. Тараса Шевченка заходів щодо підвищення рівня підготовки управлінських, журналістських та технічних кадрів для інформаційної сфери, в тому числі працівників державних органів, урахування сучасних потреб при формуванні державного замовлення на підготовку молодих фахівців.

Особливо важливою є норма даного Указу про створення Міжвідомчої комісії з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України, завданням якої координація виконання заходів щодо забезпечення формування і захисту національного інформаційного простору, безпеки у цій сфері, розроблення і підготовка проектів відповідних нормативно-правових актів.

Вже через рік Указом Президента України «Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України» від 22 січня 2002 року було затверджено Положення про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України.

У даному Положенні зазначається, що зазначена Міжвідомча комісія є консультативно-дорадчим органом, на яку покладаються такі завдання, як:

1. Аналіз стану можливих загроз національній безпеці України в інформаційній сфері та узагальнення міжнародного досвіду щодо формування та реалізації інформаційної політики;

2. Аналіз здійснення галузевих програм і виконання заходів, пов'язаних із реалізацією міністерствами та іншими центральними органами виконавчої влади державної політики в інформаційній сфері;

3. Розроблення і внесення Президентові України та Раді національної безпеки і оборони України пропозицій щодо:

- визначення національних інтересів України в інформаційній сфері, концептуальних підходів до формування державної інформаційної політики та забезпечення інформаційної безпеки держави;

- здійснення системних заходів, спрямованих на вдосконалення інформаційної політики України, реалізацію державної стратегії розвитку і захисту національного інформаційного простору та входження України у світовий інформаційний простір;
- удосконалення системи правового та наукового забезпечення інформаційної безпеки України;
- розвитку інформаційної інфраструктури держави, зокрема з питань модернізації її матеріально-технічної бази та належного фінансового забезпечення;
- організації та порядку міжвідомчої взаємодії міністерств, інших центральних органів виконавчої влади у сфері забезпечення інформаційної безпеки;
- удосконалення системи оперативного інформаційно-аналітичного забезпечення Президента України (в тому числі альтернативною інформацією) у сфері національної безпеки і оборони.

Висновки

Державна інформаційна політика - діяльність держави в інформаційній сфері, спрямована на задоволення інформаційних потреб людини і громадянина через формування відкритого інформаційного суспільства на основі розвитку єдиного інформаційного простору, цілісної держави та його інтеграції у світовий інформаційний простір з урахуванням національних особливостей і інтересів при забезпеченні інформаційної безпеки на внутрішньодержавному та міжнародному рівнях.

Інформаційна безпека виступає інструментарієм для втілення інформаційної політики, відтак державна політика інформаційної безпеки є складовим компонентом інформаційної політики держави.

Визначення основних напрямів даної політики є важливим завданням з урахуванням необхідності вироблення чітких методологічних підходів до формування системи забезпечення інформаційної безпеки. Структура даної системи є опосередкованою

В.А.ЛІПКАН.Ю. С.МАКСИМЕНКО, В. М. ЖЕЛІХОВСЬКИИ напрями державної політики інформаційної безпеки. Відтак, детермінантою і корелянтою даної системи виступає державна інформаційна політика, а не загрози інформаційній безпеці, прагнення певним чином монополізувати окремі сектори інформаційної безпеки, політичні примхи мінливої влади.

Ключові терміни та поняття

політика, державна інформаційна політика, політика інформаційної безпеки

Контрольні запитання для самоперевірки

1. *Розкрийте взаємозв'язок між поняттями «політика», «інформаційна політика», «політика інформатизації», «полі тика інформаційної безпеки».*
2. *Дайте визначення державно-правового механізму інформаційної безпеки? В чому полягають його особливості.*
3. *Які основні напрями державної політики в інформаційній сфері закріплені законодавчо?*
4. *Назвіть особливості української інформаційної політики.*
5. *Які основні нормативно-правові акти регулюють суспільні відносини інформаційної політики України? Розкрийте основні положення.*
6. *Назвіть основні завдання Міжвідомчої комісії з питань інформаційної політики та інформаційної безпеки при Раді на ціональної безпеки і оборони України.*

Завдання для самопідготовки

1. Окресліть власне бачення державної інформаційної політики України.

2. Яке місце та роль мають посідати недержавні структури в реалізації інформаційної політики країни?

Список рекомендованої літератури

Нормативні джерела

1. *Конституція* України // Відомості Верховної Ради (ВВР). - 1996. --№30.-Ст. 141.

2. Про Концепцію національної інформаційної політики: Постанова Верховної Ради України від 3 квітня 2003 року.

3. Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України: Указ Президента України від 22 січня 2002 року.

4. Про рішення Ради національної безпеки і оборони України «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної політики» від 31 жовтня 2001 року: Указ Президента України від 6 грудня 2001 року.

5. Про рішення Ради національної безпеки і оборони України «Про невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин» від 17 червня 1997 року: Указ Президента України від 21 червня 1997 року.

6. Проект Закону України про Концепцію національної інформаційної політики.

Доктринальні джерела

1. *Арістова І.В.* Державна інформаційна політика та її реалізація в діяльності ОВС України: організаційно-правові засади: Дис. д-ра. юрид. наук: 12.00.07/ Націон. ін-т внутр. справ. - Х., 2002.-408 с

2. *Арістова І.В.* Державна інформаційна політика: організаційно-правові аспекти / МВС України, Ун-т внут. справ, За заг. ред. О.М. Бандурки - Х., 2000. -366 с

3. *Беляков К.И.* Управление и право в период информатизации: Моногр. - К.: Изд.-во «КВЩ»,2001. -308 с.

4. *Ібрагімова І.* Інформаційна політика крізь призму національної безпеки // 36. наук. пр. УАДУ. - К.: Вид-во УАДУ, 2000. -Вип. 1-С. 26-40.

5. *Кормич БА.* Інформаційна безпека України: організаційно-правові основи: Навч. посібник. - К.: Кондор, 2004.- 384 с.

6. *Кормич БА.* Організаційно-правові засади політики інформаційної безпеки України: Монографія.- Одеса: Юридична література, 2003.- 472 с

7. *Литвиненко О., Чукут.С.* Інформаційна політика: Навч. посіб. -К.: Вид-во НАДУ, 2003. -ч.2. - 100 с.

8. *Макаренко Є А.* Міжнародна інформаційна політика: структура, тенденції, перспективи: Дис. д-ра. політич. наук: 23.00.04\ Київ, націон. ун-т ім. Т.Шевченка. - К., 2003. - 475 с

9. *Юдін О.К., Богуш В.М.* Інформаційна безпека держави: Навч. посібник. - Х.: Консул, 2005. - 576 с

РОЗДІЛ 5 СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Вступ

Проблема забезпечення національної безпеки в інформаційній сфері поки перебуває на стадії розроблення. Дана обставина обумовлена неадекватністю між формуванням інформаційної цивілізації і заходами із забезпечення інформаційної безпеки. У зв'язку з цим постає завдання щодо формування підходів щодо вироблення концептуального бачення інформаційної безпеки та її місця в системі національної безпеки України.

Метою даного розділу є визначення поняття «система забезпечення національної безпеки в інформаційній сфері», для досягнення якої були поставлені наступні завдання: дослідити зміст даного поняття, виявити його характерні ознаки; окреслити основний зміст та методи забезпечення інформаційної безпеки.

Інформаційна безпека забезпечується проведенням єдиної державної політики національної безпеки в інформаційній сфері, системою заходів економічного, політичного і організаційного характеру, які є адекватними загрозам та небезпекам національним інтересам особи, суспільства та держави в інформаційній сфері, а також можливостям держави п здійсненню управління ними. Система забезпечення інформаційної безпеки є інструментом реалізації державної політики інформаційної безпеки , а відтак і похідною і детермінованою напрямами державної інформаційної політики.

1. Поняття системи забезпечення інформаційної безпеки

Розділ ґрунтується на вже розробленій концепції розрізнення системи безпеки та системи забезпечення безпеки. Сказане зумовлює необхідність визначити мету функціонування даної системи.

Відсутність системи забезпечення інформаційної безпеки унеможливлює надійне забезпечення не лише інформаційної, а й національної безпеки. Головне призначення цієї системи полягає у досягненні цілей національної безпеки в інформаційній сфері, а отже основною функцією даної системи є забезпечення збалансованого існування інтересів особи, суспільства і держави в інформаційній сфері.

Система забезпечення інформаційної безпеки України (СЗІБ) створюється і розвивається відповідно до Конституції України та інших нормативно-правових актів, що регулюють суспільні відносини в інформаційній сфері. Основу даної системи складають органи, сили та засоби забезпечення інформаційної безпеки, які вживають систему адміністративно-правових, інформаційно-аналітичних, організаційно-управлінських, та інших заходів, спрямованих на забезпечення стійкого функціонування системи державного управління.

Формування СЗІБ має відбуватись за усвідомлення необхідності функціонування механізму балансу інтересів усієї системи державного управління в інформаційній сфері.

Зазначимо, що за роки незалежності в Україні лише закладено основи для формування системи забезпечення інформаційної безпеки. Так, певним чином можна говорити про напрацювання великого масиву нормативно-правових актів, де визначені основні повноваження державних органів в інформаційній сфері[9]". Президентом України вживаються активні заходи щодо вдоско-

[93] *Закон України «Про інформацію» // Відомості Верховної Ради (ВВР), 1992. - № 48. - ст. 650.; Закон України «Про електронні документи та електронний документообіг» // Відомості Верховної Ради (ВВР), 2003. - № 36. - ст. 275.; Указ Президента України від 06.12.2001 № 1193/2001 «Прорішення Ради національної безпеки і оборони України» від 31 жовтня 2001 року з питання «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки».; Закон України «Про електронний цифровий підпис» І/ Відомості Верховної Ради (ВВР), 2003. - № 36. - ст. 276.*

палення системи управління інформаційною сферою. Важливе політико-правове значення мають діючі Укази Президента України «Про деякі заходи щодо захисту держави в інформаційній сфері» (22.04.98 р.); «Про вдосконалення державного управління інформаційною сферою» (16.09.98 р.); «Про вдосконалення інформаційно-аналітичного забезпечення Президента України та органів державної влади» (14.07.2000 р.); «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі» (31.07.2000 р.); «Про додаткові заходи щодо безперешкодної діяльності засобів масової інформації, дальшого утвердження свободи слова в Україні» (09.12.2000 р.); «Про рішення Ради національної безпеки і оборони України від 19 липня 2001 року «Про заходи щодо захисту національних інтересів у галузі зв'язку та телекомунікацій» (23.08.2001р.) та ін.

Водночас функціонування даної системи не обмежується лише великим масивом нормативно-правових актів. Відтак ми не можемо констатувати про остаточне створення основних елементів системи забезпечення інформаційної безпеки. І причин тому є багато. Це і несформованість системи забезпечення національної безпеки, і невизначеність політики національної, а отже і інформаційної безпеки, і відсутність, врешті-решт, доктрини інформаційної безпеки, яка має розвивати положення Концепції національної безпеки, яка в Україні взагалі відсутня. Згодом недосконалість нормативно-правового регулювання даних процесів негативно впливає і на державне управління у даній сфері.

Нормативно-правові засади побудови, поточної діяльності та розвитку системи забезпечення інформаційної безпеки України на сьогодні складають: Конституція України, Закон України «Про основи національної безпеки України», інші законодавчі та нормативно-правові акти, що регулюють суспільні відносини в інформаційній сфері. Нормативно-правове підґрунтя має досить розвинений характер, оскільки більшість норм відповідають міжнародним стандартам, принципам і нормам забезпе-

 чення прав і свобод людини та громадянина, зокрема права на свободу слова, отримання та поширення інформації. Водночас, системні проблеми даються в знаки і при вирішенні галузевих проблем, тому не сформиваність нормативно-правової бази щодо регулювання суспільних відносин в сфері національної безпеки, відповідним чином негативно впливає на можливість формування достатньої і ефективно діючої нормативно-правової бази з питань забезпечення національної безпеки в інформаційній сфері.

У Законі України «Про основи національної безпеки України» визначено дев'ять основних напрямів державної політики національної безпеки в різних сферах життєдіяльності. До однією з них належить інформаційна, що дає усі підстави стверджувати, що інформаційна безпека є вагомою складовою національної. Водночас з незрозумілих причин автори даного закону інформаційну сферу життєдіяльності поставили на останнє місце, що свідчить про неусвідомлення значення та ролі інформаційної безпеки в розвитку і подальшому існуванні держави'".

У найбільш загальному плані під ***системою забезпечення інформаційної безпеки*** будемо розуміти систему інформаційно-аналітичних, теоретико-методологічних, адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів, спрямованих на забезпечення стійкого розвитку об'єктів інформаційної безпеки, а також інфраструктури її забезпечення.

Безперечно, можна довго дискутувати з приводу того чи іншого терміну, можна пропонувати численні варіанти, водночас змістовними вони будуть лише тоді, коли будуть визначені основи формування **і** функціонування СЗІБ.

Основами формування і функціонування системи забезпечення інформаційної безпеки є:

[94] *Логінов О.В. Сучасні проблеми забезпечення інформаційної безпеки в контексті формування системи державного управління // Науковий вісник Юридичної академії Міністерства внутрішніх справ: Збір ник наукових праць. - 2003. - № 3.- С. 199 - 204.*

- комплексне визначення поняття інформаційної безпеки та її складових елементів, світоглядне та концептуальне закріплення у концепції, доктрині, програмах, планах та інших документах;

- формування і діяльність оптимальної структури системи інформаційної безпеки, аналіз функціонування її окремих елементів, організація функціонування даної системи в цілому;

- формування єдиного методологічного підходу, а також вироблення і прийняття єдиного цілісного і узгодженого законодавства з питань інформаційної безпеки;

- створення чіткого механізму, метою якого було б координування діяльності елементів системи забезпечення інформаційної безпеки на усіх рівнях державного управління;

- підготовка і забезпечення найкращими професійними кадрами всі складові елементи підсистеми інформаційної безпеки.

За наявності даних основ можна говорити про їх системну взаємодію, яка забезпечить створення і функціонування чіткої і надійної СЗІБ.

Відповідно до основ формування молена виокремити *основні* функції системи забезпечення інформаційної безпеки України.

1. Створення та забезпечення діяльності державних та неде ржавних органів та організацій - елементів системи забезпечен ня інформаційної безпеки, що включає:

■ розроблення адміністративно-правових засад для побудови та функціонування системи інформаційної безпеки (доктрини інформаційної безпеки, організаційної та функціональної структури системи);

• системне забезпечення діяльності елементів системи: інформаційне, аналітичне, адміністративно-правове, матеріально-технічне, кадрове, ресурсне забезпечення усієї системи державного управління.

2. Управління системою інформаційної безпеки - здійснення свідомого цілеспрямованого впливу суб'єкта управління на за грози та небезпеки, внутрішні та зовнішні чинники, що вплива ють на стан інформаційної безпеки:

• розроблення на підставі доктрини інформаційної безпеки конкретних планів та технологій забезпечення інформаційної безпеки відповідно до потреб кожного рівня державного управління;

• здійснення прогнозування, планування, організації, регулювання та контролю усією системою інформаційної безпеки та окремими її елементами;

• оцінка результативності дій, витрат на проведення заходів щодо забезпечення інформаційної безпеки.

3. Здійснення планової та оперативної діяльності щодо забез печення інформаційної безпеки:

• визначення інтересів органів державного управління в інформаційній сфері та їх пріоритетності відповідно до державної інформаційної політики;

• діагностування загроз та небезпек, виявлення джерел їх виникнення, а також прогнозування можливих наслідків у разі настання із відпрацюванням відповідних превентивних заходів.

4. Міжнародне співробітництво в сфері інформаційної без пеки:

• розроблення нормативно-правової бази, що регулює інформаційні відносини між державами та їх взаємодію в галузі інформаційної безпеки;

• входження в існуючі та утворення нових двосторонніх і багатосторонніх структур (організацій), діяльність яких спрямована на розв'язання проблем інформаційної безпеки з урахуванням національних інтересів України;

• участь у роботі керівних, виконавчих та забезпечуючих підрозділів цих структур (організацій), спільне проведення пла нових таЬперативних заходів.

Звичайно, що перелік функцій не є вичерпним, водночас за їх наявності можна говорити про формування певної підсистеми, мета функціонування якої корелюватиме із загальною метою функціонування системи національної безпеки. Актуальним в контексті розглядуваних проблем вбачається про-

аналізувати зміст та призначення системи забезпечення інформаційної безпеки.

Забезпечення інформаційної безпеки досягається у процесі свідомої цілеспрямованої діяльності органів державного управління, по запобіганню можливого порушення їх нормального функціонування в результаті дії загроз та небезпек.

Метою забезпечення інформаційної безпеки є створення нормальних умов функціонування конкретного органу державного управління, а також проведення моніторингу стану інформаційної безпеки для розроблення оптимальної моделі функціонування системи забезпечення інформаційної безпеки. На дану обставину також зазначають і інші дослідники[95].

Вживаючи термін «система», і ми свідомо акцентуємо увагу на цьому, нами робиться логічний наголос на утворенні нової якості, яку складають загрози та небезпеки, суб'єкти забезпечення інформаційної безпеки. Адже структурна зв'язаність елементів системи забезпечення інформаційної безпеки є істотною її якісною характеристикою і розрив зв'язків між цими елементами може призвести до зникнення самої системи, а отже актуалізується питання забезпечення структурної єдності даної системи.

Так, наприклад, захищеність Кабінету Міністрів України і незахищеність місцевої адміністрації міста Києва у своїй сукупності не утворять стан захищеності усієї системи інформаційної безпеки органів державного управління.

Таким чином, суб'єкти системи забезпечення інформаційної безпеки України мають тісно взаємодіяти між собою, водночас кожний з них спеціалізується на вирішенні конкретних завдань відповідно до своєї предметної компетенції, вживаючи при цьому відповідні, визначені законом, адміністративно-правові фор-

[95] *Див. напр.: Левицька М.Б. Теоретике* правові аспекти забезпечення національної безпеки органами внутрішніх справ Україна: Дис...кандидата юрид. наук: 12.00.01 / Національна академія внутрішніх справ України. - К., 2002. - С 3.*

 ми та методи. У результаті такої взаємодії зазначені суб'єкти доповнюють один одного, внаслідок чого утворюють стрункy організаційно-функціональну систему, об'єднану як системою владно-розпорядчих повноважень, так і функцією по забезпеченню інформаційної безпеки. Отже, *об'єктами* системи забезпечення інформаційної безпеки України є:

- інтереси органів державного управління в інформаційній сфері;
- система органів державного управління, а також їх компетентні особи і відносини між ними (суспільні відносини в інформаційній сфері);
- власне система забезпечення інформаційної безпеки України.

2. Мета функціонування, завдання системи забезпечення інформаційної безпеки

Визначальним елементом створення будь-якої системи є її мета. Отже, очевидним є розгляд даного компоненту і при створенні системи забезпечення інформаційної безпеки України.

Виходячи з наведеного, *мета* функціонування системи забезпечення інформаційної безпеки полягає в організації управління системою інформаційної безпеки через ефективне функціонування самої системи її забезпечення. У більш загальному плані мета полягає у створенні необхідних економічних і соціокультурних умов та правових і організаційних механізмів формування, розвитку і забезпечення ефективного використання національних інформаційних ресурсів в усіх сферах життя і діяльності громадянина, суспільства й держави.

Ефективність системи державного управління національними інформаційними ресурсами та їхнім захистом значною мірою визначає загальний рівень національної безпеки, а будь-які недоліки в структурі й функціонуванні системи державного управління цими процесами призводять до непоправних збитків

суспільству й державі. Наприклад, відомо, що втрати економіки Німеччини від індустріального шпигунства перевищують 20 млрд евро на рік, втрата торгових і технічних секретів США (за неофіційними даними) обійшлась американським компаніям у 1992 році в 100 млрд доларів"[6].

Для досягнення поставленої мети на систему забезпечення інформаційної безпеки покладаються певні завдання.

Головним завданням системи забезпечення інформаційної *безпеки України* є створення умов для організації управління системою інформаційної безпеки.

До основних завдань системи забезпечення інформаційної безпеки належать:

- створення умов для забезпечення інформаційного суверенітету України;

- участь у вдосконаленні державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;

- створення умов для активного залучення засобів масової інформації до боротьби з корупцією, зловживанням службовим становищем, іншими явищами, які загрожують національній безпеці України;

- забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопу щення неправомірного втручання органів державної влади, ор ганів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;

[96] *ШаваевА.Г. Система борьбы с экономической разведкой - М.: Издательский дом «Правовое просвещение», 2000. - 236 с.*

- вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

- забезпечення інформаційної безпеки усіх складових елементів системи державного управління;

- забезпечення інформаційно-аналітичного потенціалу країни;

- реалізація державної політики інформаційної безпеки;

- ведення активної розвідувальної, контррозвідувальної і оперативно-розшукової діяльності з метою забезпечення інфор маційної безпеки для відпрацювання стратегічних, тактичних і оперативних рішень у сфері державного управління інформацій ною безпекою та вироблення механізмів їх реалізації;

- виявлення, попередження і припинення розвідувальної та іншої, спрямованої на нанесення шкоди інформаційній безпеці України, діяльності спеціальних служб, а також окремих осіб чи організацій;

- виявлення, попередження і припинення інформаційного тероризму та іншої діяльності, спрямованої на підрив функціонування системи державного управління;

- моніторинг (спостереження, оцінка і прогноз) стану інформаційної безпеки у зв'язку із впливом загроз та небезпек як зсередини, так і ззовні системи державного управління;

- протидія технічному проникненню до інформаційних системи органів державного управління з метою вчинення злочинів, проведення диверсійно-терористичної та розвідувальної діяльності;

- запобігання можливої протиправної та іншої негативної діяльності суб'єктів системи забезпечення національної безпеки зсередини системи їй на шкоду;

- забезпечення збереження державної таємниці;

- організація демократичного цивільного контролю за функ-ціонуванням системи органів державного управління тощо.

Відповідно до окресленої мети і завдань, доцільно визначити функції системи забезпечення інформаційної безпеки України.

Під **функціями системи забезпечення інформаційної** безпеки ми розуміємо здійснення суб'єктами системи забезпечення інформаційної безпеки України діяльності зі створення умов для оптимального управління системою інформаційної безпеки.

Зазначимо, що погляди щодо функцій даної системи різняться. Так, на думку *Є.Кравця,* серед основних функцій системи забезпечення інформаційної безпеки в умовах надзвичайної ситуації слід виділити: виявлення і прогнозування загроз життєво важливим інтересам об'єктів інформаційної безпеки, здійснення комплексу оперативних і довгострокових заходів для попередження та нейтралізації загроз; створення та підтримання напоготові сил і засобів забезпечення інформаційної безпеки; управління силами і засобами забезпечення інформаційної безпеки **в** умовах надзвичайної ситуації; здійснення системи заходів з відновлення нормального функціонування об'єктів інформаційної безпеки у регіонах, які потерпіли внаслідок виникнення надзвичайної ситуації; участь в заходах, покликаних забезпечувати інформаційної безпеку за межами України відповідно до міжнародних договорів та угод, укладених або визнаних українською державою[97].

Аналогічними за своїм змістом є пропоновані функції *В.Ю.Богдановичем*[98].

Ураховуючи зазначене, до **основних функцій СЗІБ** можна віднести:

• розроблення й прийняття політичних рішень, законодавчих і нормативно-правових актів щодо забезпечення системи управління національними інформаційними ресурсами та удосконалення механізмів реалізації правових норм чинного законодавства;

[97] *Кравець Є. Національна безпека України: до концепції законодавства І/ Вісн.АН України. - 1994, Ml, С.83-90.*

'■'" Богданович В.Ю. Роль та місце воєнно-політичної моделі держави у розробленні та здійсненні політики забезпечення^ воєнної безпеки // Наука і оборона. - 1999, №1, С 34-37.

• визначення і здійснення повноважень системою органів державного управління щодо оперативного управління (володіння, розпорядження, користування) державними інформаційними ресурсами;

• розроблення і реалізація організаційних заходів і нормативно-методичного забезпечення відомчих і регіональних структур в сфері формування та використання інформаційних ресурсів за умови координації діяльності згаданих структур;

• розроблення і реалізація фінансово-економічних засад регулювання процесів формування та використання інформаційних ресурсів;

• здійснення державної реєстрації інформаційних ресурсів, забезпечення повноти створення первинних і похідних інформаційних ресурсів на засадах використання інформації, що виникає (створюється) у процесі діяльності органів державного управління;

• введення технологічно та методологічно єдиних засад формування інформаційних ресурсів за результатами діяльності органів державного управління (крім інформаційних ресурсів, що мають відомості, віднесені до державної таємниці та до іншої інформації з обмеженим доступом);

■ забезпечення ефективного використання інформаційних ресурсів у діяльності органів державного управління;

• оптимізація державної політики інформатизації щодо забезпечення науково-технічних, виробничо-технологічних і організаційно-економічних умов створення та застосування інформаційних технологій, інших елементів інформаційної інфраструктури для формування, розвитку і ефективного використання інформаційних ресурсів та сприяння доступу уповноважених суб'єктів управління до світових інформаційних ресурсів, глобальних інформаційних систем;

• забезпечення функціонування ефективно діючої комплексної системи захисту інформаційних ресурсів системи органів державного управління;

• забезпечення захисту системи державного управління від хибної, спотвореної та недостовірної інформації;

• забезпечення розробки та застосування правових, організаційних і економічних механізмів стосовно форм та засобів обігу інформаційних ресурсів України (ринку інформації, інформаційних технологій, засобів обробки інформації та інформаційних послуг);

• регулювання інформаційного співробітництва, спрямо ваного на забезпечення рівноправного та взаємовигідного ви користання національних інформаційних ресурсів у процесі міжнародного обміну, здійснення єдиної державної політики наукової підтримки системи державного управління формуван ням, розвитком і використанням національних інформаційних ресурсів;

• кадрове забезпечення функціонування системи державного управління національними інформаційними ресурсами;

адміністративно-правове забезпечення функціонування системи державного управління;

• інформаційно-аналітичне забезпечення прийняття управ лінських рішень у сфері управління інформаційними ресурсами;

• контроль за встановленим порядком і правилами формування, розвитку і використання інформаційних ресурсів;

• нагляд за додержанням законодавства в сфері формування, розвитку, використання інформаційних ресурсів та здійснення правосуддя у сфері суспільних інформаційних відносин.

У межах мети завдань та функцій постає необхідність в окресленні методів і структури системи забезпечення інформаційної безпеки України.

3. Методи забезпечення інформаційної безпеки

Діяльність з забезпечення інформаційної безпеки здійснюється за допомогою різних способів, засобів і прийомів, які у своїй органічній сукупності складають методи. Метод передбачає пев-

послідовність дій на підставі конкретного плану. Методи можуть значно змінюватися і варіюватися в залежності від типу діяльності, в якій вони використовуються, а також сфери застосування.

Важливими методами аналізу стану забезпечення інформаційної безпеки є *методи опису та класифікації.* Для здійснення ефективного захисту системи державного управління слід, по-перше, описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно сформулювати систему заходів по здійсненню управління ними.

У якості розповсюджених методів аналізу стану забезпечення інформаційної безпеки використовуються методи дослідження причинних зв'язків. За допомогою цих методів виявляються причинні зв'язки між загрозами, ризиками, викликами та небезпеками; здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються заходи по їх нейтралізації. У числі даних методів причинних зв'язків можна назвати наступні: метод схожості, метод відмінності, метод сполучення схожості і відмінності, метод змін, що супроводжують, метод залишків.

Вибір методів аналізу стану забезпечення інформаційної безпеки залежить від конкретного рівня і сфери організації захисту. В залежності від загрози уможливлюється завдання щодо диференціації як різних рівнів загроз, так і різних рівнів захисту. Що стосується сфери інформаційної безпеки, то у ній, зазвичай, виділяють: фізичний, програмно-технічний, управлінський, технологічний, рівень користувача, мережний, процедурний. Розглянемо дещо детальніше кожний з цих рівнів.

На *фізичному рівні* здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються, і управлінських технологій. На *програмно-технічному* рівні здійснюється ідентифікації і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності.

 Па рівні *управління* здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях управління з боку єдиної системи забезпечення інформаційної безпеки органів державного управління. На *технологічному рівні* здійснюється реалізації політики інформаційної безпеки за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій. Па рівні *користувача* реалізація політики інформаційної безпеки спрямована на зменшення рефлексивного впливу на суб'єктів державного управління, уне-можливлення інформаційного впливу з боку соціального середовища. На рівні мережі дана політика реалізується у форматі координації дій органів державного управління, які пов'язані між собою однією метою. На *процедурному* рівні вживаються заходи, що реалізуються людьми. Серед них можна виділити наступні групи процедурних заходів: управління персоналом, фізичний захист, підтримання роботоздатності, реагування на порушення режиму безпеки, планування реанімаційних робіт.

Можна виокремити декілька типів методів забезпечення інформаційної безпеки:

• однорівневі методи будуються на підставі одного принципу управління інформаційною безпекою;

• багаторівневі методи будуються на основі декількох принципів управління інформаційною безпекою, кожний з яких слугує вирішення власного завдання. При цьому приватні технології не пов'язані між собою і спрямовані лише на конкретні чинники інформаційних загроз;

• комплексні методи - багаторівневі технології, які об'єднані до єдиної системи координуючими функціями на організаційному рівні з метою забезпечення інформаційної безпеки виходячи з аналізу сукупності чинників небезпеки, які мають семантичний зв'язок або генеруються з єдиного інформаційного центру інформаційного впливу;

• інтегровані високоінтелектуальні методи - багаторівневі, багатокомпонентні технології, які побудовані на підставі могут-

 ніх автоматизованих інтелектуальних засобів із організаційним управлінням.

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

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

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

Вельми важливим є застосування аналітичних методів пізнання і дослідження стану суспільної свідомості у сфері інформацій-

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

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

Іншим завданням захисту є забезпечення незмінності інформації під час її зберігання або передачі, тобто забезпечення її цілісності. Таким чином конфіденційність інформації, яка забезпечується за допомогою криптографічних методів не є головною вимогою при проектуванні систем захисту інформації органів державного управління. Виконання процедур криптокодування і декодування може уповільнити передачу даних та зменшити доступ до них, через те, що працівник органу державного управління буде позбавлений можливості своєчасного та швидкого доступу до цих даних та інформації, через функціонування механізму захисту. Саме тому, забезпечення конфіденційності інформації має відповідати можливості доступу до неї. Таким чином, управління в сфері інформаційної безпеки має здійснюватися на підставі принципу доступності та безпеки. Система забезпечення інформаційної безпеки в першу чергу має гарантувати *доступність і цілісність* інформації, а її конфіденційність у випадку необхідності.

Також зазначимо, що вплив хакерів та їх можливість суттєво вплинути на інформаційні системи дещо перебільшена. Здебільшого були зламані ті системи, які мали поганий захист. Так, наприклад, багато компаній в Україні, які мають солідний грошовий обіг і достатні фінансові джерела, не мають не

 те щоб цілісної системи безпеки взагалі, а й навіть окремо функціонуючої підсистеми забезпечення інформаційної безпеки. Здебільшого забезпечення інформаційної безпеки зводиться до того, що в системних блоках блокується доступ до флоппі-дисків і тим самим унеможливлюється несанкціонований запис інформації. Окрім цього, системний адміністратор встановлює спеціальні програми-фільтри, що відсіюють можливість доступу до внутрішньої мережі ззовні. Можна перераховувати й інші методи захисту інформації, водночас, нині ототожнення забезпечення інформаційної безпеки із забезпеченням безпеки комп'ютерних систем є просто концептуальною помилкою. Тому не є дивиною, що на сьогодні більша частина українських банків втратила внаслідок власної недбалості чимало коштів. І характерною рисою українського суспільства є те, що жоден з банків жодного разу не визнав факту вчиненого кіберзлочину проти себе.

У даному аспекті можна зауважити на ще одну проблему: зневага до вимог інформаційної безпеки та брак необхідних знань. Здебільшого під час робочого дня працівники, виконуючи свої службові обов'язки, відкривають паралельні вікна в Інтернеті, та самі, не усвідомлюючи того, відкривають доступ не лише до інформації, що зараз обробляється, а в цілому до комп'ютерної мережі усієї системи органів державного управління, починаючи від Кабінету Міністрів України, закінчуючи місцевими органами виконавчої влади. Отже, одним із найкращих засобів захисту інформації від нападу - не допускати його.

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

розвитку. Отже, важливим метод забезпечення інформаційної безпеки є *метод розвитку*.

Захист інформації не обмежується технічними методами, на що зазначає велике коло дослідників. Для ефективного забезпечення інформаційної безпеки важливим є різноманітні моделі та методи оцінки загроз та небезпек. їх варіативність занадто лабільна та залежить як від рівня розвитку тієї чи іншої цивілізації, так і від контексту оцінки, що проводиться, наявності всебічних даних по факторам загроз, алгоритму вирахування коефіцієнту імовірності настання та розміру негативних наслідків. Наявність конкретних даних з цього питання дозволяє досить точно визначити ступінь впливу інформаційної зброї, рівень загроз та небезпек.

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

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

Також можна зазначити на *метод моделювання,* за допомогою якого можна проводити навчання з інформаційної безпеки. Позитивний досвід цього є у США, де на базі однієї з відомих корпорацій постійно провадяться оперативно-дослідницькі навчання, щоб моделювати різні форми інформаційних атак у ході інформаційної війни. Серед методів забезпечення інформаційної безпеки важливе значення має *метод дихотомії.* Для протидії загрозам інформаційній безпеці вживаються необхідні заходи

 як в напрямку надання певного впливу на джерело загрози, так і в напрямку укріплення об'єкта безпеки. Відповідно виділяють дві предметні області протидії. Одна з них утворюється сукупністю джерел загроз, а інша - сукупністю заходів із забезпечення інформаційної безпеки органу державного управління.

Вплив на джерело загрози інформаційної безпеки спрямований на зміну чинників та умов, здатних нанести шкоду об'єкту безпеки. Метою захисту є переконання супротивника у недоцільності здійснення загроз. Що стосується органів державного управління, то джерело загроз може бути спрямовано на зміну міждержавних відносин, укріплення довіри між державами, створення умов, за яких здійснення небезпечних дій щодо об'єкта безпеки стає невигідним унаслідок виникнення небажаних наслідків або неможливим. Основним предметом за даного випадку є інформація, яка є у супротивника у вигляді відомостей, знань, оцінок. У свою чергу, інформація, що надходить від супротивника і становить собою загрозу, може бути піддана впливу для зміни її здатності завдавати шкоду, нейтралізації, трансформації або ліквідації її небезпечних властивостей. Вплив на інформаційну інфраструктуру важливий у тому випадку, коли загрозу може представляти середовище розповсюдження небезпечної інформації.

Методи впливу на інформацію у формі повідомлень можна поділити також на *електронні та неелектронні.* Електронні методи впливу застосовуються у тих випадках, коли повідомлення закріплюються на електромагнітних носіях, котрі призначені для оброблення за допомогою засобів обчислювальної техніки. Вони полягають у знищенні, викривленні, копіюванні повідомлень, які зберігаються на цих пристроях. Такі дії можуть бути вчинені лише за допомогою технічного та програмного забезпечення. Неелектронні методи за своєю суттю мають той самий зміст, але реалізуються без використання засобів обчислювальної техніки для впливу на повідомлення, закріплення на інших, передусім паперових, носіях інформації.

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

У цілому ж слід зазначити, що обрання цілей і методів протидії конкретним загрозам та небезпекам інформаційній безпеці становить собою важливу проблему і складову частину діяльності з реалізації основних напрямів державної політики інформаційної безпеки. У межах вирішення даної проблеми визначаються можливі форми відповідної діяльності органів державної влади, що потребує проведення детального аналізу економічного, соціального, політичного та інших станів суспільства, держави і особи, можливих наслідків вибору тих чи інших варіантів здійснення цієї діяльності.

Висновки

Аналіз проблем забезпечення інформаційної безпеки дав змогу зробити висновок, що найбільш важливими напрямами діяльності у цій галузі є всебічна оцінка загроз та небезпек, національної уразливості, ідентифікація критичної інфраструктури. У процесі забезпечення інформаційної безпеки важливо розуміти характер, природу, сутність і зміст загроз та небезпек, вміти своєчасно ідентифікувати джерело загрози.

Дії, пов'язані із забезпечення інформаційної безпеки, мають включати:

• спостереження, аналіз, оцінку та прогноз загроз та небезпек, критичної інфраструктури, ступеню національної уразливості;

• відпрацювання стратегії і тактики, планування попереджен ня нападу, укріплення потенційних зв'язків, вирівнювання ресурсів забезпечення інформаційної безпеки;

• відбір сил і засобів протидії, нейтралізації, недопущення нападу, мінімізації шкоди від нападу;

• дії по забезпеченню інформаційної безпеки;

• управління наслідками інциденту (кібератаки, інформаційні операції, інформаційній війни).

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

Система забезпечення інформаційної безпеки має бути міжвідомчою та ієрархічно організованою. її структура й організація має відповідати структурі державного управління з чіткою координацією дій окремих сегментів. Організація ефективної системи забезпечення інформаційної безпеки передбачає централізоване управління із конкретними відомчо-розпорядницькими функціями, які забезпечують моніторинг і контроль за усіма компонентами національного інформаційного простору. Система забезпечення інформаційної безпеки має у будь-яких ситуаціях скоординованої багатобічної і багатоаспектної інформаційної операції володіти здатністю зберігати важливі параметри свого функціонування, тобто підтримувати стан гомеостазису.

Потребують подальшого вирішення питання щодо розробки комплексу інформаційних стандартів із урахуванням забезпечення інформаційної безпеки, розвиток системи сертифікації інформаційних продуктів, систем і послуг, створення системи ліцензування діяльності організацій по окремих напрямах формування єдиного інформаційного простору України.

Ключові терміни та поняття

Система забезпечення інформаційної безпеки, сили забезпечення інформаційної безпеки, забезпечення інформаційної безпеки, система інформаційної безпеки

Контрольні запитання для **самоперевірки**

1. Поняття системи забезпечення інформаційної безпеки.

2. У чому полягає відмінність системи інформаційної безпеки від системи забезпечення інформаційної безпеки?

3. Визначте мету формування системи забезпечення інформаційної безпеки.

4. Окресліть методи забезпечення інформаційної безпеки.

Завдання для самопідготовки

1. Визначте кореляційні детермінанти формування системи забезпечення інформаційної безпеки.

2. Окресліть механізм взаємовпливу системи забезпечення інформаційної безпеки з іншими системними елементами системи національної безпеки.

Список рекомендованої літератури

Нормативні джерела

1. *Конституція* України // Відомості Верховної Ради (ВВР). -1996. -№30.-Ст. 141.

2. *Питання* Міжвідомчої комісії з питань реформування правоохоронних органів: Указ Президента України № 834/2005 від 23 травня 2005 року // www.rainbow.gov.ua/action

3. Про вдосконалення державного управління інформацій ною сферою: Указ Президента України від 16 вересня 1998 р. // Голос України. - 1998. - № 182.

4. Про вдосконалення інформаційно-аналітичного забезпе чення Президента України та органів державної влади: Указ Президента України від 14 липня 2000 р. // Урядовий кур'єр. - 2000. -№ 128.

5. Про взаємодію Служби безпеки України та органів держав ної податкової служби України з профілактики, виявлення, припинення, розкриття та розслідування злочинів, інших пра-

вопорушень у сфері розроблення, виготовлення спеціальних технічних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації та торгівлі ними: Наказ Служби безпеки України та Державної податкової адміністрації України від 9 липня 2001 ЛІ' 176/278 // Офіційний Вісник України. - 2001. - № 31. - Ст. 1432.

6. Про демократичніш цивільний контроль над Воєнною організацією і правоохоронними органами держави: Закон України від 19 червня 2003 р. // Відомості Верховної Ради. - 2003. -№46. -Ст. 366.

7. Про Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України: Указ Президента України від 6 жовтня 2000 р. // Офіційний Вісник України. -2000. -№41.

8. Про Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України: Указ Президента України від 6 жовтня 2000 р. // Офіційний Вісник України. -2000.- №41.

9. Про державну таємницю: Закон України від 21 січня 1994 р. // Відомості Верховної Ради України. - 1994. - № 16. -Ст. 93.

10. Про додаткові заходи щодо безперешкодної діяльності засобів масової інформації, дальшого утвердження свободи слова в Україні: Указ Президента України від 9 грудня 2000 р. // Урядовий кур'єр. - 2000. - № 231.

11. Про електронний цифровий підпис: Закон України від 22 травня 2003 р. // Відомості Верховної Ради. - 2003. - № 36. -Ст. 276.

12. Про електронні документи та електронний документообіг: Закон України від 22 травня 2003 р. // Відомості Верховної Ради. - 2003. - № 36. - Ст. 275.

13. Про затвердження Тимчасового регламенту Кабінету Міністрів України: Постанова Кабінету Міністрів України

від 5 червня 2000 р. // Офіційний Вісник України. - 2000. -№ 24.

14. Про захист інформації в автоматизованих системах: Закон України від 5 липня 1994 р. // Відомості Верховної Ради України. - 1994. - № 31. - Ст. 286.

15. Про заходи щодо впровадження Концепції адміністративної реформи в Україні: Указ Президента України від 22 липня 1998 р. // Офіційний Вісник України. - 1999. - № 21.

16. Про заходи щодо забезпечення інформаційної безпе ки держави: Указ Президента України від 18 вересня 2002 р. // Офіційний Вісник України. - 2002. - № 38. - Ст. 1771.

17. Про заходи щодо захисту інформаційних ресурсів держави: Указ Президента України від 10 квітня 2000 р. // Офіційний Вісник України. - 2000. - № 15.

18. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі: Указ Президента України від 31 липня 2000 р. // Урядовий кур'єр. - 2000. - № 143.

19. Про заходи щодо створення електронної інформаційної системи «Електронний Уряд»: Постанова Кабінету Міністрів України від 24 лютого 2003 р. // Офіційний Вісник України. -2003. -№9. -Ст. 378.

20. Про зміни у структурі центральних органів виконавчої влади: Указ Президента України від 15 грудня 1999 р. //Офіційний вісник України. - 1999. - №30. - Ст. 2435.

21. Про інформацію: Закон України від 2 жовтня 1992 р. // Відомості Верховної Ради України. - 1992. - №48. - Ст. 650.

22. Про Концепцію Національної програми інформатизації: Закон України від 4 лютого 1998 р. // Юрид. вісник України. -1998. -№18.- С 8-16.

23. Про ліцензування певних видів господарської діяльності: Закон України від 1 червня 2000 р. // Відомості Верховної Ради України. - 2000. - № 36. - Ст. 299.

24. Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України: Указ Президента України від 22 січня 2002 р. // Офіційний Вісник України. - 2002. - № 4. -Ст. 132.

25. Про міжнародні договори України: Закон України від 22 грудня 1993 р. // Відомості Верховної Ради України. - 2004. - № 50. -Ст. 540.

26. Про місцеві державні адміністрації: Закон України від 9 квітня 1999 р. // Відомості Верховної Ради України. - 1999. - № 20-21.-Ст. 190.

27. Про Національну комісію з питань регулювання зв'язку України: Указ Президента України від 21 серпня 2004 р. // Офіційний Вісник України. - 2004. - № 35. - Ст. 2319.

28. Про Національну програму інформатизації: Закон України від 4 лютого 1998 р. // Відомості Верховної Ради України. - 1998. -№ 27-28. - Ст. 181.

29. Про основи національної безпеки України: Закон України від 19 червня 2003 р. // Відомості Верховної Ради. - 2003. - № 39.-Ст. 351.

30. Про радіочастотний ресурс України: Закон України від 1 червня 2000 р. // Відомості Верховної Ради України. - 2000. - № 36.-Ст. 298.

31. Про Раду національної безпеки і оборони України: Закон України від 5 березня 1998 р. // Відомості Верховної Ради України. - 1998. - № 35. - Ст. 237.

32. Про рішення Ради національної безпеки і оборони України від 19 липня 2001 р. «Про заходи щодо захисту національних інтересів у галузі зв'язку та телекомунікацій: Указ Президента України від 23 серпня 2001 р. // Офіційний Вісник України. -2001. -№35. -Ст. 1622.

33. Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року з питання «Про заходи щодо

вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки»: Указ Президента України від 6 грудня 2001 р. // Офіційний Вісник України 2001. - № 50. -Ст. 2228.

34. Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 р. «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України: Указ Президента України від 6 грудня 2001 р. //Офіційний Вісник України. - 2001. - № 50.-Ст. 2228.

35. Про Службу безпеки України: Закон України від 25 березня 1992 р. //Відомості Верховної Ради. - 1992. - № 27. -Ог. 382.

36. Про телекомунікації: Закон України від 18 листопада 2003 р. // Відомості Верховної Ради України. - 2004. - № 12. -Ст. 155.

37. Про удосконалення інформаційно-аналітичного забез печення Президента України та органів державної влади: Указ Президента України від 14 липня 2000 р. // Урядовий кур'єр. - 2000.- 18 липня.

38. Про утворення Державного департаменту з питань зв'язку та інформатизації: Постанова Кабінету Міністрів України від 8 вересня 2004 р. // Офіційний Вісник України. - 2004. - № 36. -Ст. 2408.

39. Про функціональні повноваження Прем'єр-міністра України, Першого віце-прем'єр-міністра і віце-прем'єр-міністрів України: Постанова Кабінету Міністрів України від 13 грудня 2002 р. //Офіційний Вісник України. - 2002. - № 51. -Ст. 2321.

Доктринальні джерела

1. *Система* забезпечення інформаційної безпеки України. // Національна безпека і оборона. - 2001. - № 1. - С. 49 - 50..

2. *Сунь-цзы* Искусство войны: Древнейший в мире трактат о войне / Лайонел Джайлс (пер. с кит). - 2 изд. - Ростов-на-Дону: Феникс, 2003. - 288 с.

3. *Шевчук О.* Національна інфраструктура інформатизації // Зв'язок. 2000. - № 5. - С.4 - 9.

4. *Я рач кин В.И.* Информационная безопасность: Учеб. для студ. вузов, обуч. по гуманит. и соц.-экон. спец. - М.: Фонд «Мир», 2003. -640 с.

РОЗДІЛ 6
СТАНОВЛЕННЯ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Вступ

Природним еволюційним етапом цивілізаційного розвитку є входження до інформаційної ери, де основними стратегічними ресурсами є знання та інформація. Саме ці компоненти стають основою нового ~ інформаційного суспільства, яке радикально відрізняється від попередніх цивілізацій. Забезпечення інформаційної безпеки, більше того - реалізація державної інформаційної політики унеможливлюються у разі не сформованості інформаційного суспільства. Саме тому, розгляд його поняття та основних ознак є необхідним для усвідомлення глибини та системності аналізованої нами проблематики.

/. Генеза поняття «інформаційне суспільство»

Ідея інформаційного суспільства з'явилась у дослідженнях 60 - 70 рр. XX століття. Вперше термін *«інформаційне суспільство»* було використано в працях таких японських дослідників, як М. Махлуп, Т. Умесао, Й. Масуда, Т. Сакайя. Подальшого розвитку дана концепція знайшла в дослідженнях провідних американських та європейських теоретиків, а саме - Е. Тоф-флер, У. Дайзард, З. Бжезинський, М. Понятовський, Ю. Хаяші, Ж. Еллюль, Р. Коен, К. Ясперс, А. Турен, Г. Кан, Ф. Уебстер, А. Дракер, Е. Гідденс, Ч. Хенді, Л. Туроу, Дж. Гелбрайт, М. Мак-клюен, М. Порат, Т. Стоуньєр, Р. Катц, які підкреслювали значення інформаційного розвитку суспільства як нової історичної віхи цивілізації.

Синонімічними щодо інформаційного суспільства є терміни *«посткапіталістичне суспільство»* (Д. Дарендорф, П. Дрю-кер), *«постекономічне суспільство»* (В. Іноземцев, І Канн),

«технотронне суспільство» (З. Бжезінський), *«постмодер нізм»* (Б.Турен, Б.Старт), *«постіндустріальне суспільство»* (Д.Белл, Т.Стоунєр).

Масштабний рівень наукових розроблень формування інформаційного суспільства дозволив дійти висновку про важливість не тільки інформації, але й знань. Саме це викликало появу в наукових колах інших синонімічних термінів щодо інформаційного суспільства таких, як «інтелектуальне суспільство», «суспільство знань», «цифрове суспільство», «суспільство мереже-ного інтелекту» тощо.

У рамках ідеології інформаційного суспільства існують різні напрямки та тенденції, які розглядають нові соціальні перспективи - можливі, бажані або негативні: від позитивних можливостей державного управління економікою, створення законодавчої бази для вільного доступу міжнародної спільноти до інформації - до запобігання загрозі політичного контролю за націями з використанням високих технологій та розшаруванням спільнот на «золотий мільярд і безправну периферію».

Побудова інформаційного суспільства є стратегічною метою провідних держав світу - США, Японії, Канади, а також країн-членів Європейського Союзу. Розуміючи актуальність та важливість розвитку інформаційно-технічної сфери як запоруки конкурентоспроможності, все більше країн обирають аналогічну стратегію, зокрема й Україна.

Цікавою є думка *Гурковського В І.,* який вважає, що напевно, якщо йдеться про нову стадію розвитку суспільства, її доцільно визначати на основі аналізу зміни продуктивних сил і виробничих відносин. З цього погляду інформаційне суспільство можна було б розглядати як суспільство, в якому основним предметом праці переважної більшості людей стають інформація й знання, тобто інформаційні ресурси, знаряддям праці - комп'ютерна техніка, засобами - інформаційні технології. У розвинутих країнах уже сьогодні існуючі суспільні відносини багато в чому визначаються саме цією обставиною. Відповідно і економіка суспільства

орієнтована на виробництво, насамперед, продуктів інформаційної, інтелектуальної діяльності, що пов'язані із виробленням нової інформації і нових знань, з перетворенням їх у стан, зручний для використання іншими людьми, та продажем цих продуктів як товару.

Не можна не погодитись і *зАріст овою І.В.,* що перехід до інформаційного суспільства - це найбільш раціональний шлях підвищення якості життя населення країни за рахунок вступу України на новий шлях цивілізованого розвитку і переходу економіки на наукоємні, ресурсозберігаючі виробництва. Підставами для такого переходу є постійний рух країни від комп'ютеризації (у 60-х - **80-х** рр.) до інформатизації (у 80-х - 90-х рр.) і створення розвиненого інформаційного середовища суспільства (на рубежі століть).

2. Поняття інформаційного суспільства

Визначення поняття «інформаційне суспільство» є доволі дискусійним в наукових колах. Як правило науковці намагаються окреслити основні, фундаментальні ознаки такого суспільства.

Здебільшого, суспільство вважається інформаційним, якщо:

1. Будь-хто, будь-де й у будь-який час можуть одержати за відповідну плату чи безкоштовно на основі автоматизованого доступу і систем зв'язку будь-яку інформацію і знання, необхідні для їхньої життєдіяльності і рішення особистих і соціально значущих задач.

2. У суспільстві виробляється, функціонує і доступна будь-якому індивіду, групі чи організації сучасна інформаційна технологія.

3. Існують розвинені інфраструктури, що забезпечують створення національних інформаційних ресурсів у обсязі, необхідному для підтримки науково-технологічного й соціально-історичного прогресу, що постійно прискорюється.

4. Відбувається процес прискореної автоматизації й роботизації всіх сфер і галузей виробництва та керування.

5. Здійснюються радикальні зміни соціальних структур, наслідком яких є розширення сфери інформаційної діяльності та послуг.

В.М. Бражко, О.М. Гальченко, В.С. Цимбалюк визначають *інформаційне суспільство* як:

1. Суспільство, в якому більшість працівників займаються створенням, зібранням, відображенням, реєстрацією, накопиченням, збереженням і поширенням інформації, особливо її найвищої форми - знань;

2. Суспільство, в якому діяльність людей ґрунтується на використанні послуг, що надаються за допомогою інформаційних технологій та технологій зв'язку.

Одразу зазначимо, що становлення інформаційного суспільства має об'єктивний характер, хоча значної актуальності надається питанню державного управління цим процесом.

Юдін О.К. та Богуш В.М. зазначають про необхідність розроблення *програми входження в інформаційне суспільство,* під якою розуміють план діяльності держави з реалізації Концепції національної інформаційної політики, спрямованої на вирішення завдань формування інформаційної сфери, які забезпечують:

- розвиток засобів масової інформації;
- формування інформаційних ресурсів;
- надання інформаційних послуг;
- підготовку інформаційних продуктів;
- прийняття термінових заходів, спрямованих на створення єдиного інформаційного простору держави і його інтеграції в світовий інформаційний просіір;
- встановлення жорсткого контролю за державними системами зв'язку та телекомунікацій.

Програма повинна передбачати розгляд таких напрямків:

- формування і розвиток інформаційної інфраструктури де ржави;

- реалізація права на інформацію в інформаційних мережах;
- захист особистості, суспільства, держави від неякісної, фальшивої інформації і дезінформації;
- захист інтелектуальної власності в інформаційних мережах;
- захист інформації, в тому числі персональних даних, даних в інформаційних мережах;
- застосування можливостей інформаційних технологій для розвитку нових форм трудової діяльності, освіти та виховання;
- захист прав споживачів та розвиток конкуренції в мережах;
- міжнародне співробітництво з проблем створення глобального інформаційного суспільства;
- координація робіт з реалізації програми.

У 1993 р. сутність інформаційного суспільства була розкрита Комісією ЄС: *«Інформаційне суспільство* - це суспільство, в якому діяльність людей здійснюється на основі використання послуг, що надаються за допомогою інформаційних технологій та технологій зв'язку» [198]. На думку Європейської Комісії, інформаційним суспільством слід вважати [197]:

- суспільство нового типу, що формується внаслідок глобальної соціальної революції та породжується вибуховим розвитком і конвергенцією інформаційних та комунікаційних технологій;
- суспільство знання, тобто суспільство, в якому головною умовою добробуту кожної людини і кожної держави стає знання, здобуте завдяки безперешкодному доступу до інформації та вмінню працювати з нею;
- глобальне суспільство, в якому обмін інформацією не буде мати ні часових, ні просторових, ні політичних меж; яке, з одного боку, сприятиме взаємопроникненню культур, а з іншого - відкриватиме кожному співтовариству нові можливості для самоідентифікації.

Вважається, що в майбутньому існуватиме декілька типів інформаційного суспільства, як колись існувало декілька моделей індустріального суспільства. Ключовими ознаками для

визначення типу суспільства будуть такі: ступінь забезпечення рівних прав доступу громадян до основного ресурсу - інформації, ступінь участі у житті суспільства та самореалізації людей із обмеженими фізичними можливостями.

Ґрунтовним є визначення інформаційного суспільства, запропоноване *Арістовою І.В.:* «Громадянське суспільство з розвинутим інформаційним виробництвом і високим рівнем інформаційно-правової культури, в якому ефективність діяльності людей забезпечується розмаїттям послуг на основі інтелектуальних інформаційних технологій та технологій зв'язку».

Важко не погодитись з дослідницею, яка зазначає, що сьогодні в Україні ані держава, ані комерційний сектор економіки повною мірою не визначити своєї позиції і своїх стратегічних цілей інформаційної політики в умовах становлення та розвитку інформаційного суспільства. Ті концепції і програми, що є, вирішують ряд, хоча і важливих, але приватних завдань цього напрямку.

На нашу думку, загальнодержавна концепція повинна враховувати умови, за яких жорсткі механізми, що забезпечують уніфікацію та єдине централізоване управління всією інформаційно-телекомунікаційною інфраструктурою, зруйновані, а нові, що засновані на економічній та суспільній необхідності та створені на основі ринкових стимулів, ще не працюють повною мірою. Обсяги українського ринку інформаційних продуктів та послуг не можна порівняти із ринками розвинених західних країн. Необхідна його структурна реорганізація та модернізація, що потребує значних інвестицій. Вважаємо, що необхідно більш чітко визначити, що повинна робити держава, а що - ринкові структури. Процес розподілу відповідальності та власності між державою і ринком в інформаційній сфері ще не здобув сталих рис. Співвідношення держава - ринок для України дещо інше, ніж у країнах з прозорою ринковою економікою. Ринкові стимули поки що не в змозі забезпечити відтворення інформаційних ресурсів і технологій. Концепція державної інформаційної політики в Україні повинна

виходити з цього положення, а не копіювати у всьому загальні підходи зарубіжних країн, що скеровані на удосконалення ринкових відносин, що вже давно існують, і механізмів у галузі створення та використання інформаційно-комунікаційних технологій.

Найбільшого успіху на шляху до інформаційного суспільства досягають країни, у яких держава формує і активно проводить у життя відповідну цілеспрямовану політику. Роль держави постає у створенні сприятливих умов для розвитку цього процесу, до яких можна віднести:

- максимальне залучення ресурсів (кадрових, фінансових, матеріальних і ін.) до інформаційного виробництва;
- нормативно-правове та нормативно-технічне регулювання;
- підтримка проектів і програм, які демонструють можливості інформаційного суспільства;
- розвиток міжнародного інформаційного обміну та співробітництва.

3. Побудова інформаційного суспільства в Україні

Інформаційне суспільство в Україні задеклароване в розділі 13 Програми інтеграції України в Європейський Союз. Відповідно до цієї Програми розвиток інформаційного простору в нашій країні визначається як станом інформаційних технологій (програмно-технічні засоби доступу до інформації, телекомунікаційна складова тощо), так і кількісним та якісним складом доступних на ринку інформаційних продуктів.

У 1998 р. Верховною Радою України розроблено й законодавчо затверджено «Національну програму інформатизації України», у вересні 1993 року Уряд прийняв «Комплексну програму створення єдиної національної системи зв'язку», а також важливого значення має прийняття Закону України «Про Національну систему конфіденційного зв'язку України» у 2002 році тощо.

Україна є членом низки міжнародних організацій зв'язку та інформатизації - Всесвітнього поштового союзу (ВПС), Міжна-

 родного союзу електрозв'язку (МСЕ), а також регіональних європейських організацій - Європейської конференції адміністрацій зв'язку (СЕРЇ), Європейського інституту телекомунікаційних стандартів (ETS1).

Оскільки Україна визначила курс на євроінтеграцію, то вона має брати до уваги найкращі взірці та стратегії розвитку країн-членів Європейського Союзу у всіх напрямках життєдіяльності суспільства, зокрема у інформаційно-технічній сфері. Саме тому, реалізація стратегії становлення інформаційного суспільства ЄС знаходить своє відображення у відповідних спільних документах Україна - ЄС.

Так, у липні 1994 року було підписано Протокол про наміри між Державним комітетом зв'язку та інформатизації і Генеральним Директоратом XIII (в подальшому Генеральний Директорат ЄС з проблем інформаційного суспільства), який заклав на офіційному рівні підвалини для спільних дій в сфері інформаційного суспільства.

Подальшого розвитку положення даного Протоколу відобразились в Меморандумі про взаєморозуміння між Генеральним Директоратом з питань інформаційного суспільства Європейської Комісії і Державним комітетом зв'язку та інформатизації України щодо розвитку інформаційного суспільства, який був підписаний 14 вересня 2000 року.

Як зазначається в Меморандумі, Євросоюз та Україна погодились співпрацювати з метою розвитку інформаційного суспільства в Україні, визнаючи важливість цього для розвитку ефективної ринкової економіки та для забезпечення можливостей якісного працевлаштування.

Українська сторона підтвердила свій намір розвивати програму e-Ukraine, яка відповідає потребам українського суспільства, стимулювати розвиток послуг інформаційного суспільства в Україні. В свою чергу, Гендиректорат з питань Інформаційного суспільства буде надавати поради, які базуються на досвіді, отриманому в рамках програми e-Europe, та надаватиме можливість

Україні брати участь у відповідних заходах кожного разу, коли це буде доцільно. Гендиректора'!' також зобов'язався надавати поради у відповідь на запити з приводу стратегій Інформаційного суспільства, розроблених в Україні, а також надавати експертну та технічну допомогу згідно з існуючими процедурами та правилами.

21 вересня 2005 року відбулись Парламентські слухання з питань розвитку інформаційного суспільства в Україні, в яких взяли участь народні депутати України, представники центральних органів державної влади, провідні вчені та фахівці.

Основною метою цих слухань є сформування пропозицій, рекомендацій, які могли стати планом дій при прийнятті довгострокової програми розвитку інформаційного суспільства, незалежної від змін в уряді, парламенті та Президента тощо.

Акцентувалась увага на тому факті, що відсутність послідовної державної політики в Україні, спрямованої на побудову інформаційного суспільства, вже призвела до відставання від інших країн, а також сучасне інформаційне суспільство та його наступна фаза - суспільство, побудоване на знаннях, окрім технологічного, набуло багато вимірів: гуманітарного, мас-медійного, культурологічного, освітньо-наукового та інших. Для створення цілісної моделі такого суспільства і власне економіки знань та індустрії інтелектуальних інформаційних технологій Україні необхідно паралельно розбудовувати дві фази інформаційного суспільства: перша - прискорити побудову інформаційної та телекомунікаційної інфраструктури країни шляхом залучення зовнішніх та внутрішніх інвестицій; розширення конкурентного середовища серед провайдерів Інтернету та мобільного зв'язку; охоплення органів державного управління та провідних державних інституцій; друга - одночасно мобілізувати науку, освіту, промисловість, гуманітарну, мас-медійну сфери і бізнес на пріоритетних напрямах розвитку інформаційного суспільства, побудованого на знаннях.

Така стратегія дозволила б Україні побудувати розвинене інформаційне середовище, конкурентноспроможну індустрію ін-

телектуальних інформаційних технологій та власну економіку знань, стати повноправним членом міжнародної світової кооперації у створенні глобального інформаційного суспільства.

Арістова І.В. виділила наступні головні характеристики розвитку інформаційного суспільства в Україні:

1. У 90-ті рр. в Україні утворився комерційний інформаційний сектор економіки, структура якого та зайнятість у якому ще не достатньо досліджені.

2. Поширюється процес інформатизації комерційного сектору економіки. Інформатизація в бізнесі йде за модернізаційною схемою.

3. В Україні присутні головні рушійні сили розвитку інформаційного суспільства, що позначені експертами Європейського Союзу:

- реклама та пропаганда привабливого сучасного способу жит тя: електронне листування, торгівля і банківські операції, резер вування подорожей, домашні читання школярів і курсові роботи студентів; послуги Інтернет та інші послуги доступні тільки тим, у кого є персональний комп'ютер;
- велика кількість електронних ігор розрахована на дітей, які завтра потенційно стануть проповідувати можливості інфор маційних і телекомунікаційних технологій на роботі;
- комп'ютеризація освіти - її вплив сьогодні не такий великий, проте завтра під впливом конкуренції, зростання комп'ютерної письменності батьків і вимог самих учнів, також: під впливом розвитку мережевих послуг вона збільшуватиме соціальну роль інформаційних і телекомунікаційних технологій;
- подальше зниження цін на різноманітні інформаційні та те- лекомунікаційні технології (ІТТ), що передбачено експертами, слугує рушійною силою розвитку інформаційного суспільства;
- комфорт і зручність у будинку, офісі, в машині завжди були і залишаються важливою рушійною силою соціальних змін;
- все більша кількість людей та організацій використовують електронні пристрої для особистої охорони та безпеки;

- можливість більш широкої участі сільського населення в економічному та соціальному житті за допомогою ІТТ також стимулює розвиток інформаційного суспільства.

4. У країні почалася «домашня комп'ютерна революція», тобто збільшення рівня зацікавленості до ІТТ.

Таким чином, аналіз науково-практичних та нормативно-правових джерел свідчить, що пріоритетним завданням інформаційної політики України є створення[1] інформаційного суспільства як запоруки розвитку соціально-економічного життя населення та вирішенню ряду глобальних проблем сучасності.

При чому слід розуміти, що не всі країни одночасно зможуть досягти такого рівня розвитку суспільства, яке можна буде характеризувати як інформаційне. Це обумовлено великої прірвою у рівнях розвитку процесів інформатизації між найбільш розвинутими країнами та країнами третього світу, з перехідною економікою. Більше того, процеси інформатизації слугують каталізаторами розвитку в інших сферах суспільного життя (політичних, економічних, культурних тощо), а тому розрив цей не тільки не зменшується, а дедалі більше зростає.

Висновки

Інформаційне суспільство являє собою певну асоціацію країн, що досягли відповідних економічних, культурних і соціальних параметрів розвитку, зокрема, високого рівня інформатизації життя громадян і суспільства, управління державою, розвитку науки, освіти й культури, а також володіють значним ступенем інтегрованості у світову економіку.

Основними *характеристиками інформаційного суспільства* є: інформаційна економіка, індустрія інформаційних послуг, сучасні інтелектуальні інформаційні технології та технології зв'язку, значний потенціал науки, потреба фізичних та юридичних осіб в інформації, високий рівень інформаційно-правової

 культури всіх суб'єктів інформаційних відносин, матеріально-технічне забезпечення різноманітних послуг.

Зрозуміло, що процес становлення інформаційного суспільства в Україні є довготривалим, багатоетапним, складним, але він є необхідним з огляду на світові тенденції та обрану зовнішньополітичну стратегію.

Ключові терміни та поняття

інформаційне суспільство, програма входження держави в інформаційне суспільство, безпека інформаційного суспільства

Контрольні запитання для самоперевірки

1. *Назвіть основних розробників теорії інформаційного суспільства.*

2. *У чому полягає сутність та зміст інформаційного суспільства? Дайте визначення поняттю «інформаційне суспільство».*

3. *Назвіть особливості інформаційного суспільства в Україні.*

4. *Чим регламентована і в чому полягає взаємодія ЄС та України в сфері побудови інформаційного суспільства?*

5. *Що таке програма входження в інформаційне суспільство? Розкрийте її основні положення.*

Завдання для самопідготовки

1. Окресліть основні ознаки інформаційного суспільства.
2. Шляхи інформаційного суспільства в Україні.

Список рекомендованої літератури

Нормативні джерела

1. Конституція України // Відомості Верховної Ради (ВВР). -1996.-№30.-Ст. 141.

2. Питання Воєнної доктрини України: Указ Президента Ук раїни № 702/2005 від 21 квітня 2005 року // www.rainbow.gov. ua/action

3. Питання забезпечення діяльності Національної системи конфіденційного зв'язку: Указ Президента України від 4 липня 2002 року.

4. Питання Міжвідомчої комісії з питань реформування правоохоронних органів: Указ Президента України № 834/2005 від 23 травня 2005 року // www.rainbow.gov.ua/action

5. Про затвердження Державної програми створення, розвитку та забезпечення функціонування Національної системи конфіденційного зв'язку Постанова Кабінету Міністрів України від 11 жовтня 2002 року.

6. Про Комплексну програму створення єдиної національної системи зв'язку Постанова Кабінету Міністрів України від 23 вересня 1993 року.

7. Про Концепцію розвитку зв'язку України до 2010 року: Постанова Кабінету Міністрів України від 9 грудня 1999 року.

8. Про Національну систему конфіденційного зв'язку Украї ни: Закон України // Відом. Верховної Ради України. - 2002. - № 15-Ст.ЮЗ.

9. Про Програму інтеграції України до Європейського Союзу: Указ Президента України від 14 вересня 2000 року.

Доктринальні джерела

1. *Арістова І.В.* Державна інформаційна політика та її реалізація в діяльності ОВС України: організаційно-правові засади: Дис. д-ра. юрид. наук: 12.00.07/ Націон. ін-т внутр. справ. - Х., 2002.-408 с

2. *Белл Д.* Грядущее постиндустриальное общество: Опыт социального прогнозирования / Пер. с англ. В. Иноземцев. - **М.:** Academia, **1999.** - 956 с.

3. *Братченко ИЛ.* Мифы и реалии информационного обще ства: вверх по лестнице... - СПб.: Терра, **2001. - 429 с.**

4. *Брижко В.М., Галъченко О.М., Цимбалюк В.С.* і ін. Інформаційне суспільство. Дефініції: людина, її права, інформація, інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція. - К.: Інтеграл, 2002. - 220 с

5. *Брижко В.М., Галъченко О.М., Цимбалюк В.С.* і ін. Інформаційне суспільство. Дефініції: людина, її права, інформація, інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція. - К.: Інтеграл, 2002. - 220 с

6. *Гурковсъкий В.І.* Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: Дис. канд. юрид. наук \ 25.00.02 - К., 2004. - 225 с

7. *Макаренко ЄА.* Міжнародна інформаційна політика: структура, тенденції, перспективи: Дис. д-ра. політич. наук: 23.00.04\ Київ, націон. унт ім. Т.Шевченка. - К., 2003. - 475 с

8. *Меморандум* про взаєморозуміння між Генеральним Директоратом з питань інформаційного суспільства Європейської Комісії і Державним комітетом зв'язку та інформатизації України щодо розвитку інформаційного суспільства від 14 вересня 2000 року.

9. *Міжнародний* конгрес «Інформаційне суспільство в Україні: стан, проблеми, перспективи /Матеріали конгресу. - К.: НТУ «КШ».-328с.

10. *Парламентські* слухання з питань розвитку інформацій ного суспільства в Україні від 21 вересня *2005 року.*

11. *Ракитов* А.И. Философия компьютерной революции. - М.: Политиздат, 1991. - 287 с.

12. *Юдін О.К., Богуш В.М.* Інформаційна безпека держави: Навч. посібник. - Х.: Консул, 2005. - 576 с.

13. *Ялта-2000.* Роль Європи у XXI столітті //Матеріали міжнародної наукової конференції, 7-9 травня 2000 р. - К.: Видавничий центр «Київський університет», 2000. - 286 с

РОЗДІЛ 7
ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ У СФЕРІ ПРАВ І СВОБОД ЛЮДИНИ

Вступ

Забезпечення інформаційної безпеки охоплює три аспекти:

1) інформаційно-технічну безпеку - управління потенційними чи реальними загрозами з метою захисту комп'ютерних, телекомунікаційних технологій та інших технологій зв'язку;

2) інформаційно-психологічну безпеку - управління реальними чи потенційними загрозами, що можуть завдати шкоди психіці людини, суспільства;

3) інформаційну безпеку у сфері прав і свобод людини - управління реальними чи потенційними загрозами з метою забезпечення права на інформацію.

Тому актуальним, з огляду на акцент дослідження, - євроінтеграційний поступ України — є аналіз інформаційної безпеки у сфері прав і свобод людини.

1. Поняття права на інформацію

Забезпечення захисту прав і свобод людини в інформаційній сфері є однією з найважливіших цілей інформаційної безпеки, адже права і свободи людини у сфері інформації є ключовими інститутами громадянського суспільства, правової, демократичної держави, надбанням і цінністю європейської спільноти.

Дана думка підтверджується доповіддю Уповноваженого Верховної Ради України з прав людини *Н.Карпачової,* яка зазначила, що світова практика демократичного державотворення переконує в тому, що право на свободу думки і слова, на вільне виявлення своїх поглядів і переконань є одним з наріжних каменів розбудови демократичної, правової держави і громадянського суспільства.

На думку *Арістової І.В.,* у літературі висловлюються погляди, в яких право громадян на інформацію - лигне складова частина свободи слова та преси, або, навпаки, свобода інформації -умовне позначення цілої групи свобод і прав: свободи слова або свободи вираження думок; свободи преси та інших ЗМІ; права на одержання інформації, що має суспільне значення; свободи поширення інформації.

Вважається, що право на інформацію не охоплюється цілком свободою слова і преси. Воно значно багатіше, змістовніше і має власну субстанцію, грає свою роль у задоволенні певних інтересів суб'єктів; тому зрізаність даного найважливішого права необгрунтовано. Навряд чи виправданий і такий, надмірно широкий, підхід до змісту права на інформацію. Аргументом на користь таких висловлень є, безумовно, законодавча практика найвищого рівня - конституційна. Йдеться, наприклад, про ст. 34 Конституції України, де закріплені не лише свобода думки, слова, але і право на інформацію. Зовсім не випадково закріплені свобода думки і слова та право на інформацію в різних частинах, хоча й однієї статті. Тим самим підкреслюється як їхній взаємозв'язок і взаємопроникнення, так і відома автономність, самостійність, «суверенність».

Взагалі, вперше поняття *«право на інформацію»* було визначено у ст. 9 Закону України «Про інформацію» від 2 жовтня 1992 року, а саме: «Всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій».

Причому, ст. 1 цього Закону визначає *інформацію* як «документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі». Але після набрання чинності Законом «Про телекомунікації», де в Прикінцевих положеннях говориться про необхідність узгодження чинного законодавства з поло-

женнями цього нового Закону, поняття інформації визначається вже як відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Досить цікавим є також такі основні положення, що закріплюються відповідними нормами Закону «Про інформацію»:

1. Громадяни мають право доступу до інформації про них, а в період збору інформації мають право знати, які відомості про них і з якою метою збираються, а також оспорювати правильність, повноту, доцільність такої інформації.

2. Право на інформацію охороняється законом.

3. Держава гарантує усім учасникам інформаційних відносин рівні права та можливості доступу до інформації.

4. Інформація не може бути використана з метою, що завдає шкоди правам та свободам громадян України.

5. Не підлягають розголошенню відомості, які становлять державну чи іншу передбачену законом таємницю.

6. Реалізація права на інформацію громадянами, юридичними особами і державою не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи та законні інтереси інших громадян, права та інтереси юридичних осіб.

7. Коленому громадянину забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, перед бачених законами України.

З прийняттям Конституції України в 1996 році, ***право людини на інформацію*** - самостійне конституційне право, яке дозволяє людині вільно збирати, зберігати, використовувати і поширювати інформацію будь-яким способом, що гарантується ч. 2 ст. 34 Конституції України.

Здійснення цього права може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформа-

 ції, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя (ч. 3 ст. 34 Конституції України).

Комплекс прав та свобод в інформаційній сфері вважається непорушним та невідчужуваним. За основу положень розділу II «Права, свободи та обов'язки людини і громадянина» Конституції України взято ряд міжнародних нормативно-правових актів. Зокрема, Загальна декларація прав людини, Міжнародний пакт про економічні, соціальні і культурні права, Міжнародний пакт про громадянські та політичні права.

У цілому ст. 34 Конституції України відповідає ст. 19 Міжнародного пакту про громадянські і політичні права, який надає кожній людині право вільно шукати, одержувати і поширювати будь-яку інформацію та ідеї, незалежно від державних кордонів, та в будь-який спосіб за своїм вибором.

2. Види інформаційних прав і свобод і їх зв'язок з іншими правами та свободами людини та громадянина

Крім загального визначення права людини на інформацію в ст. 34 Конституції, є ряд інших інформаційних прав і свобод, що закріплюються конституційними нормами.

1. *Свобода особистого і сімейного життя* (ст. 32: «...не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини»);

2. Таємниця листування, телефонних переговорів, телеграфної й іншої кореспонденції (ст. 31: «...винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо»);

3. Право громадянина не зазнавати втручання в його особисте та сімейне життя, шляхом збирання, зберігання, вико ристання та поширення конфіденційної інформації про особу без її згоди, знайомитися в органах державної влади, органах місцевого самоврядування, установах та організаціях із відо мостями про себе (ст. 32: це відноситься до відомостей, що «не є державною або іншою захищеною законом таємницею»);

4. Право громадянина направляти індивідуальні або колективні письмові звернення або особисто звертатися в органи державної влади, органи місцевого самоврядування та до посадо вих і службових осіб цих органів (ст. 40);

5. Право кожного громадянина на сприятливе навколишнє середовище, достовірну інформацію про її стан (ст. 50: «...така інформація ніким не може бути засекречена»);

6. Право кожного на свободу творчості і право доступу до культурних цінностей (ст. 54: результати інтелектуальної, творчої діяльності громадянина «ніхто не може використовувати або поширювати їх без його згоди, за винятками, встановленими законом»);

7. *Право кожного громадянина на одержання кваліфікованої правової допомоги* (ст. 59: «…у випадках, передбачених законом, ця допомога надається безоплатно»).

Деякі конституційні положення, також мають відношення до інформаційних прав і свобод.

Так, за статтями 21, 24 усі люди є вільні і рівні у своєму *праві на інформацію,* яке є невідчужуваним та непорушним і не залежить від раси, кольору шкіри, релігійних та інших переконань, статі, етнічного та соціального походження тощо.

Без отримання необхідної інформації, вільного її використання людина не змогла б розвивати свою особистість (ст. 23).

Право на інформацію пов'язане з *правом на свободу світогляду і віросповідання,* яке включає свободу сповідувати будь-яку релігію або не сповідувати ніякої, безперешкодно відправляти

одноособово чи колективно релігійні культи і ритуальні обряди, вести релігійну діяльність (ст. 35).

Реалізація *права на освіту* (ст. 53) неможлива без вільного інформаційного обміну між людьми. Процес навчання означає, перш за все, пошук і отримання необхідної інформації.

Ст. 34 Конституції можна також розглядати як певний розвиток і конкретизацію положення ч. 3 ст. 15, що забороняє здійснення в Україні цензури, тобто обмежувальних заходів щодо здійснення свободи слова в засобах масової інформації. Вона гарантує духовну і творчу свободу, не обмежену ніякою обов.'язковою ідеологією. Положення статті гарантують доступ до засобів масової інформації політичним партіям і рухам, громадським організаціям, профспілкам, кожній окремій людині. Ніхто не може бути примушений до зміни чи висловлювання своїх поглядів і переконань.

Зрозуміло, що Конституція України закріплює основний зміст прав і свобод в інформаційній сфері, але їх конкретизація відображається в ряді інших нормативно-правових актах, а саме таких як: Закон У РСР «Про мови в Українській РСР» від 28.10.1989 р., Закон України «Про науково-технічну інформацію» від 25.06.1993 р., Закон України «Про інформаційні агентства» від 28.02.1995 р., Закон України «Про Концепцію Національної програми інформатизації» від 04.02.1998 р., Закон України «Про захист інформації в автоматизованих системах» від 05.07.1994 р., Указ Президента «Про додаткові заходи щодо безперешкодної діяльності ЗМІ, дальшого утвердження свободи слова в Україні» від 9.12.2000 р., Указ Президента «Про вдосконалення державного управління інформаційною сферою» від 16.09.1998 р., Розпорядження Президента «Про додаткові заходи поліпшення інформаційної діяльності» від 5.10.1998 р. тощо.

Великого значення мають Рішення Конституційного Суду України (КСУ) у справі про офіційне тлумачення положення частини першої статті 7 Цивільного кодексу Української РСР

(справа про поширення відомостей) від 10 квітня 2003 р., Рішення КСУ у справі щодо офіційного тлумачення ст. 3, 23, 31, 47, 48 Закону України «Про інформацію» та ст. 12 Закону України «Про прокуратуру» (справа К.Г.Устименка) від ЗО жовтня 1997 р. та Цивільний кодекс України.

Як зазначають дослідники даної проблематики конституційне закріплення права на інформацію ще не робить зрозумілим механізм його реалізації. Це стосується, наприклад, надання відповідної інформації державними органами і органами місцевого самоврядування за запитами громадян. Крім розробки чіткого та прозорого механізму здійснення права на доступ до різного роду інформації, її отримання, поширення, використання тощо, необхідно також внести зміни до чинного законодавства у зв'язку з дуже бурхливим розвитком сучасних інформаційних технологій та мереж, зокрема Інтернет, зробити ревізію застарілих законодавчих визначень і понять, приділити серйозну увагу узгодженню національного законодавства з міжнародними нормами і стандартами в інформаційній галузі».

3. Структура конституційного права на інформацію

Структура конституційного права на інформацію, що закріплюється Конституцією України та Цивільним кодексом України, визначається такими складовими як:

- збирання інформації;
- зберігання інформації;
- використання інформації;
- поширення інформації.

Відповідно до Закону України «Про інформацію», структурою вищезазначеного права є:

- одержання;
- зберігання;
- використання;
- поширення.

Поняття «збирання» інформації, яке міститься у тексті Конституції, законодавчо не визначено, оскільки Закон України «Про інформацію» дає дефініції тільки таким поняттям як «одержання», «зберігання», «використання» та «поширення».

Під *одержанням* інформації законодавець розуміє набуття, придбання, накопичення інформації громадянами, юридичними особами або державою відповідно до чинного законодавства України.

Зберігання інформації — означає забезпечення належного стану інформації та її матеріальних носіїв.

Використання інформації — задоволення інформаційних потреб громадян, юридичних осіб і держави.

Поширення інформації - розповсюдження, обнародування, реалізацію інформації у встановленому законом порядку.

Цікавим є той факт, що даний Закон у ст. 38 закріплює також «право власності на інформацію», під яким розуміється «врегульовані законом суспільні відносини щодо володіння, користування і розпорядження інформацією». Отже, законодавець оперує такими поняттями, як «володіння», «користування», «розпорядження», які не визначені законодавчо.

Тому, більшість науковців наголошують на необхідності уточнення понять «користування» і «розповсюдження» для з'ясування чіткої різниці між «використанням» і «користуванням» та між «поширенням» і «розповсюдженням» інформації, оскільки фактично використання інформації передбачає і збирання, і поширення інформації, і взагалі будь-які інші маніпуляції з нею.

Особливої уваги для забезпечення інформаційної безпеки, заслуговує поняття «доступу до інформації».

Ст. 28 Закону України «Про інформацію» містить поняття «режим доступу до інформації» як передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації.

Основними положеннями цього Закону згідно зі статтями 28, 29, ЗО, що закріплюють режим доступу до інформації, є:

1. За режимом доступу інформація поділяється на відкриту та інформацію з обмеженим доступом.

2. Держава здійснює контроль за режимом доступу до інформації.

3. Завдання контролю за режимом доступу до інформації полягає у забезпеченні додержання вимог законодавства про інформацію всіма державними органами, підприємствами, установами та організаціями, недопущенні необґрунтованого віднесення відомостей до категорії інформації з обмеженим доступом.

4. Державний контроль за додержанням встановленого режиму здійснюється спеціальними органами.

5. У порядку контролю Верховна Рада України може вимагати від урядових установ, міністерств, відомств звіти, які містять відомості про їх діяльність по забезпеченню інформацією зацікавлених осіб.

6. Будь-яке обмеження права одержання відкритої інформації забороняється Законом.

7. Інформація з обмеженим доступом поділяється на конфіденційну і таємну.

8. До *конфіденційної інформації* належать відомості, що знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб, які можуть поширюватися за їх бажанням відповідно до передбачених ними умов.

9. *Таємною* є інформація, що містить відомості, які становлять державну та іншу, передбачену Законом таємницю, розголошення якої завдає (чи може завдати) шкоди особі, державі, суспільству.

Відповідно до вимог ст. 37 Закону України «Про інформацію» не підлягають обов'язковому наданню для ознайомлення за інформаційними запитами офіційні документи, які містять інформацію:

- визнану у встановленому порядку державною таємницею;
- конфіденційну;
- про оперативну та слідчу роботу органів прокуратури, МВС, СБУ, роботу органів дізнання та суду у тих випадках, коли її розголос може зашкодити оперативним заходам, розслідуванню чи дізнанню, порушити право людини на справедливий та об'єктивний судовий розгляд її справи, створити загрозу життю або здоров'ю будь-якої особи;
- що стосується особистого життя громадян;
- щодо внутрівідомчої службової кореспонденції, якщо вона пов'язана з розробкою напряму діяльності установи, з процесом прийняття рішень і передує їх прийняттю;
- що не підлягає розголошенню згідно з іншими законодавчими актами;
- фінансових установ, підготовлену для контрольно-фінансових відомств.

Зазначимо, що критерії віднесення інформації до таємної, порядок її обігу та захисту регулюються Законом України «Про державну таємницю» від 21 січня 1994 р. Зміст відомостей, які належать до державної таємниці, викладений у «Зводі відомостей, що становлять державну таємницю України (ЗВДТ)», який у 1995 р. був затверджений наказом Держкомітету України з питань державних секретів.

Досить важливим є розкриття такого поняття як «комерційна таємниця». Так, відповідно до Закону України «Про підприємства в Україні» під *комерційною таємницею підприємств* розуміють відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами тощо, що не є державними таємницями, розголошення (передача, витік) яких може завдати шкоди його інтересам.

Склад і обсяг відомостей, що становлять комерційну таємницю, порядок їх захисту визначаються керівником підприємства (відповідно до Листа Головної державної податкової інспекції України від 23.11.1995 року).

Оскільки ч. 2 ст. 32 Конституції України забороняє збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, то досить цікавим є розгляд цієї проблеми детальніше.

Ст. 23 Закону України «Про інформацію» містить такі основні норми:

1. Основними даними про особу (персональними даними) є національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження.

2. Джерелами документованої інформації про особу є видані на її ім'я документи, підписані нею документи, а також відомості про особу, зібрані державними органами влади та органами місцевого і регіонального самоврядування в межах своїх повноважень.

3. Забороняється збирання відомостей про особу без її попередньої згоди, за винятком випадків, передбачених законом.

Офіційне тлумачення статті 23 надано Конституційним Судом України у його Рішенні № 5-зп від **30.10.97,** де персональні дані про особу віднесені до конфіденційної інформації.

4. Правове забезпечення реалізації права на інформацію

Доволі дискусійним з точки зору забезпечення інформаційної безпеки України є Указ Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Internet і забезпечення широкого доступу до цієї мережі в Україні» від 31 липня 2000 року.

З одного боку, цей Указ закріпив, що з метою розвитку національної складової глобальної інформаційної мережі Internet, забезпечення широкого доступу громадян до цієї мережі, ефективного використання її можливостей для розвитку вітчизняної науки, освіти, культури, підприємницької діяльності, зміцнення міжнародних зв'язків, належного інформаційного забезпечення для здійснення органами державної влади та органами

 місцевого самоврядування своїх повноважень, повнішого задоволення потреб міжнародного співтовариства в об'єктивній, комплексній інформації щодо різних сфер суспільного життя в Україні, а також вирішення інших завдань, визначених в Посланні Президента України до Верховної Ради України «Україна: поступ у XXI сторіччя. Стратегія економічного та соціального розвитку на 2000 - 2004 роки», необхідно встановити, що розвиток національної складової глобальної інформаційної мережі Internet, забезпечення широкого доступу до цієї мережі громадян та юридичних осіб усіх форм власності в Україні, належне представлення в ній національних інформаційних ресурсів є одним з пріоритетних напрямів державної політики в сфері інформатизації, задоволення конституційних прав громадян на інформацію, побудови відкритого демократичного суспільства, розвитку підприємництва.

У зв'язку з чим, основними завданнями розвитку національної складової мережі Internet і забезпечення широкого доступу до цієї мережі в Україні визначено:

1) створення у найкоротші строки належних економічних, правових, технічних та інших умов для забезпечення широкого доступу громадян, навчальних закладів, наукових та інших установ і організацій усіх форм власності, органів державної влади та органів місцевого самоврядування, суб'єктів підприємницької діяльності до мережі Інтернет;

2) розширення і вдосконалення подання у мережі Internet об'єктивної політичної, економічної, правової, екологічної, науково-технічної, культурної та іншої інформації про Україну, зокрема тієї, що формується в органах державної влади та органах місцевого самоврядування, навчальних закладах, наукових установах та організаціях, архівах, а також бібліотеках, музеях, інших закладах культури, розширення можливостей для доступу в установленому порядку до інших національних інформаційних ресурсів, постійне вдосконалення способів подання такої інформації;

3) забезпечення конституційних прав людини і громадянина на вільне збирання, зберігання, використання та поширення інформації, свободу думки і слова, вільне вираження своїх поглядів і переконань;

4) забезпечення державної підтримки розвитку інфраструктури, надання інформаційних послуг через мережу Інтернет; створення умов для розвитку підприємницької діяльності та конкуренції у галузі використання каналів електронного зв'язку, створення можливостей для задоволення на пільгових умовах потреб у зазначених послугах навчальних закладів, наукових установ та організацій, громадських організацій, а також бібліотек, музеїв, інших закладів культури, закладів охорони здоров'я, включаючи розташовані у сільській місцевості;

5) розвиток та впровадження сучасних комп'ютерних інформаційних технологій у системі державного управління, фінансовій сфері, підприємницькій діяльності, освіті, наданні медичної та правової допомоги тощо;

6) вирішення завдань щодо гарантування інформаційної безпеки держави, недопущення поширення інформації, розповсюдження якої заборонено відповідно до законодавства;

7) вдосконалення правового регулювання діяльності суб'єктів інформаційних відносин, виробництва, використання, поширення та зберігання електронної інформаційної продукції, захист прав на інтелектуальну власність, посилення відповідальності за порушення встановленого порядку доступу до електронних інформаційних ресурсів усіх форм власності, за навмисне поширення комп'ютерних вірусів;

8) забезпечення вступу України до відповідних міжнародних організацій, що займаються питаннями розвитку телекомунікаційних систем; захист прав на інформацію; протидія поширенню інформації, яка завдає шкоди людині і громадянину, суспільству і державі; внесення в установленому порядку відповідних пропозицій; сприяння залученню коштів міжнародної технічної

допомоги, використання можливостей міжнародних програм для розвитку в Україні мережі Internet.

З іншого боку, на основі вже згадуваного Указу Президента створено Департамент спеціальних телекомунікаційних систем та захисту інформації СБУ, який повинен контролювати увесь обіг інформації в органах державної влади, організаціях, на підприємствах, незалежно від форм власності, що використовують мережі передачі даних, зокрема Інтернет, тим самим, порушуючи основні права і свободи людини в інформаційній сфері, закріплені Конституцією. Дещо виправило ситуацію виведення даного департаменту зі складу СБУ у 2006 році.

Слід зазначити, що деякі з існуючих нормативних актів суперечать один одному чи взагалі застаріли, внаслідок чого почасти виникають колізії . Відсутність чітких демократичних правових засад, неточність, а часом відсутність офіційного визначення широковживаних термінів у цій галузі гальмує її розвиток в цілому, що саме по собі є загрозою національним інтересам в інформаційній сфері.

Висновки

1. За умови, коли основні інформаційні права та свободи людини і громадянина закріплені у всіх перерахованих документах і однакові за своїм змістом, то підстави їх можливого обмеження і прямі обмеження, що визначені там же, найчастіше не збігаються між собою.

2. Керуючись принципом пріоритету норм міжнародного права над національним законодавством, варто підготувати уніфікований перелік засад для обмежень і випадків прямого обмеження прав і свобод із наступним внесенням змін у Конституцію України і міжнародні акти.

3. В усіх розглянутих документах прямо вказується, що обмеження інформаційних прав і свобод можуть бути встановлені тільки законом, причому не передбачається дозвільний принцип

реалізації зазначених прав і свобод, коли основні інформаційні права і свободи можна буде реалізовувати тільки у встановлених чиновниками випадках. Усі підстави для обмежень можна зводити до трьох груп: для захисту інтересів особистості, забезпечення стабільності в суспільстві, а також в інтересах національної безпеки.

Ключові терміни та поняття

право на інформацію, інформаційні права та свободи, права і свободи в інформаційній сфері, структура права на інформацію, одержання, використання, поширення, зберігання інформації, режим доступу до інформації, конфіденційна інформація, таємна інформація, комерційна таємниця

Контрольні запитання для самоперевірки

1. Дайте визначення поняття «право на інформацію».

2. Як співвідносяться поняття «право на інформацію», «інформаційні права» ?

3. Яка структура конституційного права на інформацію?

4. Назвіть основні права та свободи в інформаційній сфері, що закріплюються Конституцією України.

5. Охарактеризуйте Указ Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Internet і забезпечення широкого доступу до цієї мережі в Україні» від 31 липня 2000 року.

6. Що Ви вважаєте слід зробити для створення надійної системи забезпечення інформаційної безпеки і захисту інформаційної сфери суспільства?

Завдання для самопідготовки

1. Розкрийте зміст основних інформаційних прав та свобод.

2. Сформуйте модель нормативно-правових актів, які регулюють суспільні відносини в сфері інформаційних прав і свобод людини..

Нормативні джерела

1. *Конституція* України // Відомості Верховної Ради (ВВР). -1996. -№30. -Ст. 141.

2. Про державну таємницю: Закон України від 21 січня 1994 року.

3. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Internet і забезпечення широкого доступу до цієї мережі в Україні: Указ Президента України від 31 липня 2000 року.

4. Про інформацію: Закон України від 2 жовтня 1992 року.

Цоктринальні джерела

1. *Арістова І .В.* Державна інформаційна політика та її реалізація в діяльності ОВС України: організаційно-правові засади: Дис. д-ра. юрид. наук: 12.00.07/ Націон. ін-т внутр. справ. - Х., 2002.-408 **с**

2. *Карпачова Н.І.* Стан дотримання та захисту прав і свобод в Україні: Перша щорічна доповідь Уповноваженого Верховної ради України з прав людини. - К., 2000. - С. 202.

3. *Кормич БА.* Організаційно-правові засади політики інформаційної безпеки України: Монографія.- Одеса: Юридична література, 2003. - 472 **с**

4. *Кушакова Н.В.* Конституційне право на інформацію в Україні (порівняльний аналіз): Дис. ... канд.,юрид.наук: 12.00.02 / Київ.націон.. ун-т ім.. Т.Шевченка. -К., 2003. - 243 **с**

5. *Макаренко Є А.* Міжнародна інформаційна політика: структура, тенденції, перспективи: Дис. д-ра. політич. наук: 23.00.04 / Київ, націон. ун-т ім. Т.Шевченка. - К., 2003. - 475 **с**

РОЗДІЛ 8
ІНФОРМАЦІЙНА БЕЗПЕКА ЄВРОПЕЙСЬКОГО СОЮЗУ

Інформаційна безпека становить собою складову інформаційної політики держави, відтак, її розгляд є необхідним для розуміння тих процесів, які відбувається в Євросоюзі, прийомів та методів забезпечення інформаційної безпеки, нормативно-правової бази, що регулює суспільні відносини в даній сфері.

1. Коріння європейської єдності

Використовуючи засоби економічного, інформаційного, політичного та міжнародно-правового впливу, глобалізація суттєво змінює розуміння концепції суверенної національної держави, оскільки все прогресуючу роль в управлінні державотворчим процесом покладається на наднаціональні утворення.

Ще два десятиріччя тому, відомий американський футуролог *Е. Тоффлер* у роботі «Третя хвиля» зазначив, що цивілізація Третьої хвилі базуватиметься на новій системі розподілу влади, в якій нація як така втрачатиме своє значення, більш важливу роль відіграватимуть інші інститути, які виникнуть не стільки за географічною ознакою, скільки за культурною, релігійною, екологічною чи економічною.

Не дивлячись на все зростаючу взаємозалежність світу, стирання державних кордонів, можна констатувати появу нового критерію поділу держав, поділу на основі не тієї чи іншої національно-державної приналежності, а на основі технічної оснащеності, інформаційною розвиненості.

У Посланні Президента України до Верховної Ради України «Європейський вибір. Концептуальні засади стратегії економічного та соціального розвитку України на 2002 - 2011 роки» визначено, що курс на європейську інтеграцію є природним наслідком здобуття Україною державної незалежності. Він

викристалізовується з історії нашого народу, його ментальності та демократичних традицій, з прагнення нинішнього покоління бачити свою державу невід'ємною складовою єдиної Європи. Європейський вибір України - це водночас і рух до стандартів реальної демократії, інформаційного суспільства, соціально орієнтованого ринкового господарства, базованого на засадах верховенства права й забезпечення прав та свобод людини і громадянина.

Вагоме значення має інша законодавчо закріплена норма, яка зазначила, що Україна має створити ефективну систему інформаційного захисту своїх національних інтересів, що передбачає проведення активної інформаційно-аналітичної роботи, спрямованої на роз'яснення своєї внутрішньої і зовнішньої політики, формування прихильного ставлення до України в парламентських, урядових і неурядових колах, збирання інформації про наміри або акції, що плануються щодо України з метою своєчасного і адекватного на них реагування, прогнозування перспективних напрямів міжнародної активності.

Головна функція зовнішньої політики України в цьому контексті полягає у подоланні штучної інформаційної ізоляції навколо неї та донесенні до України світових інформаційних потоків, забезпеченні політичних, договірно-правових та організаційно-технічних можливостей включення вітчизняних інформаційних служб в міжнародну систему обміну інформацією.

Протягом 90-х років XX ст. Європейський Союз (ЄС) став найвпливовішою інтеграційною структурою на європейському континенті, відіграючи важливу роль в забезпеченні європейської безпеки-

Взагалі, ***ідея європейської єдності*** мала давнє коріння у суспільно-політичному розвитку Європи. Серед апологетів даної ідеї можна відзначити видатних миелителей та філософів XIX століття, таких як Е. Крюсе, В- Пени, Дж. Мадзіні, В.Ф. Генц та Й. К. Блунтшлі, Й. Альтузіус, Ш.-Л. Монтеск'є, Ж. Ж. Руссо, П. Ж. Прудон, Дж. Бентам, Р. Кобден, Ф. Ліст та К. Франц.

Особливої активності дана ідея набула у 20-х роках XX ст. у наукових та філософських трактатах Р. Куденхове - Калергі, Е, Мейрігп, Ж. Бенд, П. Валері, К. Сфорц та А. Тріан, які відстоювали позицію необхідності створення Об'єднаних Штатів Європи в якості самостійного потужного політичного та економічного союзу, спроможного протистояти натиску союзу Англії та Америки.

Тривалий час ці теоретичні розробки мали виключно теоретичний характер. Лише після Першої та Другої світової війни на порядку денному для європейців став пошук засобів забезпечення безпеки та попередження нового збройного конфлікту, оскільки було зрозуміло, що держава сама по собі втратила свою природну роль - гаранта національної безпеки, а тому необхідно винайти таку систему безпеки, такий політичний механізм, який зміг би попередити загрозу нового конфлікту та відновити зруйновану економіку регіон"'.

Деякі аспекти історичної ідеї об'єднаної Європи знайшли своє відбиття в основоположних установчих документах Європейського Союзу: Договору про заснування Європейського об'єднання вугілля та сталі (ЄОВС) від 18 квітня 1951 р., Договору про заснування Європейського Економічного Співтовариства (ЄЕС) та Європейського Співтовариства з атомної енергії (Євроатом) від
25 березня 1957 р., Єдиному Європейському Акту, підписаному в Люксембурзі 17 лютого 1986 р, та в Гаазі 28 лютого 1986 р., в Маастрихтському Договору про Європейський Союз від 7 лютогр 1992 року з подальшими змінами та доповненнями, запровадженими Амстердамським від 2 жовтня 1997 року та Ніццьким від
26 лютого 2001 р. договорами.

Преамбула Договору про заснування Європейського Економічного Співтовариства визначає, що *метоfа європейської інтегра-*

[99] *Снігир О.В, Україна у геополітичних концепціях Європейського Союзу: динаміка «об'єкт -суб'єктних» відносин: Дис... канд.. політ. Наук: 21.01.01 / Національний інститут стратегічних досліджень. - К.,2004,178с.,С.62*

ції є більш тісний союз європейських народів, який досягається шляхом спільних дій, спрямованих на усунення бар'єрів, що розділяють Європу. Актуальною для України є теза про те, що інші народи Європи, які поділяють їх ідеал, повинні приєднуватися до їх зусиль.

Не менш актуальною є інше положення, юридично закріплене в Декларації про майбутнє Європейського Союзу від 15 грудня 2001 р., відповідно до якого єдиний кордон, який проводить Європейський Союз, - це кордон демократії та прав людини. Союз є відкритим тільки для країн, що поважають основоположні цінності, такі як вільні вибори, дотримання прав меншин і правова держава"[100].

Виходячи зі змісту установчих договорів Європейського союзу, особливу увагу він приділяє розвитку спільної політики в таких сферах, як *економічна, з вугілля та сталі та з атомної енергії,* що прямо витікає з установчих договорів (Договір про заснування Європейського об'єднання вугілля та сталі, Договір про заснування Європейського Економічного Співтовариства та Європейського Співтовариства з атомної енергії), *зовнішня політика та політика безпеки,* а також *співробітництва поліцій і судів в кримінально-правовій сфері (в галузі юстиції та внутрішніх справ).*

Саме Маастрихтський договір запровадив поняття «трьох опор», кожна з яких тотожна вищезазначеним сферам. Важливість даного нормативно-правового акта підтверджується ще й тим, що вперше були закріплені загальна зовнішня політики та політика безпеки країн ЄС, а саме:

- захищати загальні цінності, основні інтереси та незалежність Союзу;
- зміцнювати безпеку Союзу та держав-членів усіма способами;

[100] *Декларація про майбутнє Європейського Союзу, прийнята Європейською Радою в Лакені 15 грудня 2001 р.*

- підтримувати мир та зміцнювати міжнародну безпеку згідно з принципами Статуту ООН, Гельсінського заключного акту та цілями Паризької хартії;

- сприяти міжнародному співробітництву;

- розвивати та консолідувати демократію й законність, пова гу до прав людини й основних свобод *"".*

Отже, Євроінтеграція має досить динамічний характер. Якщо раніше союз європейських країн мав за мету створення виключно єдиного економічного простору, то наразі особливої актуальності набуває розвиток «другої» та «третьої» опор - зовнішня політика і політика безпеки та співробітництво поліцій і судів в кримінально-правовій сфері відповідно.

У зв'язку з рівнем інформаційно-технічного розвитку Євросо-юзу, особливого значення в діяльності ЄС має проблема забезпечення інформаційної безпеки.

Спільна позиція країн-членів Європейського Союзу щодо змісту поняття «інформаційна безпека» була висловлена представником Швеції при обговоренні питань міжнародної інформаційної безпеки на 56-й сесії Генеральної Асамблеї ООН, згідно з якою *інформаційна та мережева безпека* означає захист особистої інформації про відправників і одержувачів, захист інформації від несанкціонованих змін, захист від несанкціонованого доступу до інформації і створення надійного джерела постачання обладнання, послуг та інформації.

Інформаційна безпека також охоплює захист інформації, що стосується військового потенціалу та інших аспектів національної безпеки. Недостатній захист життєво важливих інформаційних ресурсів та інформаційних і телекомунікаційних систем може створити загрозу міжнародній безпеці.

Позиція з приводу інформаційної безпеки відзначається раціоналізмом, адже предметом безпеки називаються конкретні поняття різних видів інформації. Крім того, простежується досить чітке розмежування особливостей *інформаційної безпеки*

"" Договор об Европейском союзе 1992 г. - Страсбург, 1992-С. 19.

 (особиста інформація, інформаційне забезпечення життя суспільства) та *інформаційної безпеки держави* (інформаційне забезпечення національної безпеки).

2. Боротьба з кіберзлочинністю

У рамках інформаційного забезпечення національної безпеки, захисту особистої інформації є боротьба з кіберзлочинністю, оскільки це особливо актуальна проблема для країн Європи, що обумовлено високим рівнем комп'ютерної оснащеності різних сфер життєдіяльності суспільства.

Статті 29, 34 Договору про заснування Європейського Союзу, Директива Парламенту і Ради 95/46/ЕС від 24/10/1995 «Про захист приватних осіб у галузі обробки персональних даних та щодо вільного руху таких даних»; Регламент Парламенту і Ради ЄС № 45/2001 від 18/12/2000 «Про захист фізичних осіб у сфері обробки особистої інформації інституціями і органами Співтовариства та про вільний рух такої інформації», Резолюція Ради ЄС «Про законний моніторинг телекомунікацій» (96/3 329/01) від 17 січня 1995 р.- це лише частина нормативно-правових актів Європейського Союзу, що порушують питання боротьби з комп'ютерною злочинністю.

Базовим міжнародним нормативно-правовим документом, що регулює суспільні відносини у сфері боротьби з кіберзлочинністю, є Конвенція Ради Європи «Про кіберзлочинність» від 23 листопада 2001 року.

Європейський Союз лише готується до імплементації Конвенції. Першими кроками на цьому шляху були Спільна Позиція 1999/364/JHA від 27 травня 1999 року, затверджена Радою ЄС на підставі ст. 34 Договору про заснування ЄС щодо переговорів відносно проекту Конвенції про комп'ютерну злочинність, які відбулися у Раді Європи, та Пропозиції для Рамкового Рішення Ради ЄС щодо атак, спрямованих на інформаційні системи.

Цікавим є той факт, що, аналізуючи нормативно-правові акти ряду країн Європейського союзу, відповідно до яких закріплена відповідальність за передбачені даною Конвенцією діяння, найбільше відповідає конвенціальним нормам Кримінальний кодекс Німеччини.

Отже, відповідно до цієї Конвенції комп'ютерні правопорушення класифіковані на певні групи. *Перша група* передбачає кримінальну відповідальність за вчинення правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, а саме:

1) незаконний доступ;
2) нелегальне перехоплення;
3) втручання у дані;
4) втручання у систему;
5) зловживання пристроями.

Друга група передбачає відповідальність за правопорушення, пов'язані з комп'ютерами, а саме:

1) підробка, пов'язана з комп'ютерами;
2) шахрайство, пов'язане з комп'ютерами.

Третя група - правопорушення, пов'язані зі змістом інформації, а саме правопорушення, пов'язані з дитячою порнографією:

1) вироблення дитячої порнографії з метою її розповсюдження за допомогою комп'ютерних систем;
2) пропонування або надання доступу до дитячої порнографії за допомогою комп'ютерних систем;
3) розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем;
4) набуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи;
5) володіння дитячою порнографією у комп'ютерній системі чи на комп'ютерному носії інформації.

Четверта група включає правопорушення, пов'язані з порушенням авторських та суміжних прав.

 До речі, положення даної Конвенції знайшли своє відображення в Законі України «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України» від 23.12.2004 року, відповідно до якого в розділі 16 «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» викладені у новій редакції статті 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку), ст. 362 (Несанкціоновані дії з інформацією, яка обробляється в електронно - обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчиненні особою, яка має право доступу до неї), ст. 363 (Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється) Кримінального кодексу України та передбачена кримінальна відповідальність за статтями 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут), 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) та 363 - 1 (Перешкоджання роботі електронно- обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку).

3. Регулювання Інтернет-відносин у країнах Європи

Цікавим з точки зору інформаційної безпеки є досвід регулювання Інтернет - відносин деяких європейських країн. Як

зазначає *Макаренко Є.Л.,* у більшості європейських країнах прийняті (або існують в проекті) закони, що дають можливість притягнути до відповідальності провайдерів хостових послуг за розміщення на їхніх сайтах інформації незаконного змісту; деякі правила обмежують доступ провайдерів до таких джерел інформації. Мережеві оператори не можуть бути притягнуті до відповідальності за зміст інформації, яка передається мережами, однак вони зобов'язані на умовах виданих ліцензій вжити необхідних заходів щодо користувачів і клієнтів, які використовують мережі для передання інформації незаконного змісту. В країнах ЄС також існує практика самоврегулювання хостових послуг: наприклад, у Великій Британії (Фонд «Безпечна Мережа»), у ФРН і Нідерландах прийняті кодекси поведінки та створені незалежні органи самоврегулювання, які розробляють етичні стандарти для змісту інформації та класифікації незаконної інформації. Класифікація інформації незаконного змісту викладена так:

1) використання телекомунікаційних засобів для поширення образливої чи непристойної інформації користувачами підліткового віку (до 18 років);

2) свідоме надання телекомунікаційних послуг для поширення незаконної інформації відповідно до пункту 1;

3) свідоме надання інтерактивних комп'ютерних послуг незаконного змісту;

4) свідоме використання телекомунікаційних засобів для здійснення правопорушення відповідно до пункту 3.

Німеччина прийняла Закон про інформаційні і комунікаційні послуги (1997 р.), в якому визначений статус цифрового підпису, внесені поправки до Карнега кодексу, в закони про авторські права та обмеження на морально шкідливу для молоді інформацію.

Правове регулювання інформації в Інтернет, згідно з доповіддю Міністерства економіки, фінансів та промисловості Франції, повинно:

1) забезпечити свободу комунікації он-лайн;

2) визначити обов'язки постачальників послуг (зокрема, видавців та посередників);

3) запровадити захист інтелектуальної власності в режимі онлайн;

4) забезпечити ефективне регулювання змісту інформації, що є в мережі Інтернет;

5) забезпечити захист персональних даних;

6) забезпечити правовий статус доменів;

7) забезпечити вільний доступ до масивів інформації в мережі Інтернет для масового використання.

З цією метою Франція подала до Європейської Ради ЄС меморандум з пропозицією розширити доступ до Інтернету і створити регулятивні механізми для діяльності в мережі.

4. Співвідношення положень нормативно-правових актів Європи та України, що регулюють відносини у сфері інформаційних прав та свобод людини і громадянина

Іншим цікавим моментом у контексті аналізу проблем забезпечення інформаційної безпеки Євросоюзу є розгляд основних нормативно-правових актів, що закріплюють права та свободи громадян Євросоюзу в інформаційній сфері.

Основним документом Європейського Союзу, що закріплює такі права громадян є **Хартія основних прав Європейського Союзу** від 7 грудня **2000** року.

Хартія проголошує, що права, які в ній закріплюються, базуються на конституційних традиціях та загальних міжнародних зобов'язаннях держав-членів, а також Договору про Європейський Союз, Договору про Європейські співтовариства, Європейській конвенції про захист прав людини та основних свобод, Соціальних хартіях, прийнятих Європейським співтовариством й

Радою Європи та судової практики суду Європейських співтовариств і Європейського суду з прав людини.

Аналіз даного документу, дозволяв виокремити ряд прав та свобод людини в інформаційній сфері в контексті інформаційної безпеки Європейського Союзу, що практично повторюють положення Конституції України.

Так, ст. 3 даного Договору зазначає, що кожна людина має *право на фізичну недоторканність та недоторканність психі ки.* Отже, дана теза корелює з таким національним інтересом людини в інформаційній сфері, як забезпечення права людини на захист від маніпуляції індивідуальною свідомістю та таким конституційним положенням, яке закріплено в статті 34 Конститу ції України, відповідно до якого кожному гарантується право на свободу думки та слова, на вільне вираження своїх поглядів і переконань.

Ст. 7 закріплює положення, відповідно до якого кожна люди -на має *право на повагу її приватного та сімейного життя, на недоторканність житла та таємниці кореспонденції.*

Згідно зі ст. 8 кожна людина має *право на охорону відомостей особистого характеру.*

Таким чином, дані норми віддзеркалюються у ст. 31 Конституції України, а саме: кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, а також ст. 32 - ніхто не може зазнавати втручання в його особисте і сімейне життя. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Ст. 11 визначає, що кожна людина має *право на свободу вира жати свою думку.* Це право охоплює свободу підтримувати свою думку, отримувати та розповсюджувати інформацію та ідеї без будь-якого втручання з боку публічних властей та незалежно від державних кордонів. Забезпечується свобода та плюралізм

 засобів масової інформації. Основна ідея даної тези закріплена Конституцією України в статтях 15 (Суспільне життя в Україні ґрунтується на засадах політичної, економічної та ідеологічної багатоманітності. Жодна ідеологія не може визнаватися державою як обов'язкова. Цензура заборонена.) та 34 (Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір.).

Ст. 17 закріплює *охорону інтелектуальної власності.* Саме ця теза корелює з такими конституційними нормами, визначеними у ст. 41 (Кожен має право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності.) та ст. 54 (Громадянам гарантується свобода літературної, художньої, наукової і технічної творчості, захист інтелектуальної власності, їхніх авторських прав, моральних і матеріальних інтересів, що виникають у зв'язку з різними видами інтелектуальної діяльності. Кожний громадянин має право на результати своєї інтелектуальної, творчої діяльності; ніхто не може використовувати або поширювати їх без його згоди, за винятками, встановленими законом).

Ст. 41 зазначає, що кожна людина має *право на доступ до матеріалів, що мають до неї безпосереднє відношення, при забезпеченні законних інтересів конфіденційності, а також професійної і комерційної таємниці.* Ст. 34 Конституції України відображає основну ідею вищезазначеної статті, а саме: кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Кожен має право збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб — на свій вибір. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших лю-

дей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Насамкінець, відповідно до ст. 42 кожен громадянин чи громадянка Європейського Союзу, чи будь-яка фізична чи юридична особа, яка проживає чи має офіційно зареєстроване місцеперебування в одній з держав-членів, має *право доступу до документів Європейського парламенту, Ради та Європейської комісії.* Що ж до України, то ст. 3 Конституції України закріпила, що держава відповідає перед людиною за свою діяльність.

Висновки

Українські та європейські національні інтереси людини в інформаційній сфері є схожими, що ще раз доводить про вірність обраного нашою державою євроінтеграційного шляху.

Резюмуючи вищевикладене, зазначимо, що сучасний етап становлення громадянського суспільства визначається входженням України до провідних технологічно розвинутих країн світу, до глобального інформаційного простору. Саме тому ми маємо використовувати досвід таких країн, що вже мають досить серйозні напрацювання у сфері забезпечення інформаційної безпеки, зокрема досвід Європейського Союзу.

Ключові терміни та поняття ***інформаційна безпека Європейського Союзу, кіберзлочин-ність, основні права та свободи в інформаційній сфері Євро-союзу***

Контрольні запитання для **самоперевірки**

1. Дайте визначення поняття «інформаційна безпека Євро-союзу».

2. Розкрийте історію становлення Європейського Союзу.

3. Назвіть основні права та свободи в інформаційній сфері, що закріплюються Хартією основних прав Європейського Союзу від 7 грудня 2000 року.

4. Як співвідносяться права та свободи в інформаційній сфері, що закріплюються Хартією основних прав Європейського Союзу від 7 грудня 2000 року між правами та свободами в інформаційній сфері, закріпленими Конституцією України?

5. Які заходи запроваджені Євросоюзом для боротьби з кібер-злочинністю?

Завдання для **самопідготовки**

1. Розкрийте зміст заходів по забезпеченню інформаційної безпеки країнами Європи.

2. Окресліть критерії співвіднесення законодавства України та ЄЄ, що регулює суспільні відносин и в інформаційній сфері.

Список рекомендованої літератури

Доктринальні джерела

1. *Макаренко ЄЛ.* Міжнародна інформаційна політика: структура, тенденції, перспективи: Дис. д-ра. політич. наук: 23.00.04\ Київ, націон. ун-т ім. Т.Шевченка. - К., 2003. - 475 с.

2. *Маркое Б.В.* Демократия и интернет. Технологии информационного общества - Интернет и современное общество // Материалы Всероссийской объединенной конференции (20-24 ноября **2000** г.) - СПб., **2000.** - 292 с.

3. *Снігир О.В.* Україна в геополітичних концепціях Європейського Союзу: динаміка «Об'єкт — суб'єктних» відносин: Дис. ... канд. політич. наук: 21.01.01\ Націон. ін.- т стратегіч. досліджень. -К., 2004. - 178 с.

4. *Тоффлер Э.* Третья волна: Пер. с англ. / Э.Тоффлер. - М.: ООО «Издательство АСТ», 2002. - 776 с.

Інтернет ресурси

1. www.rada.gov.ua // Європейський вибір. Концептуальні засади стратегії економічного та соціального розвитку України на 2002 — 2011 роки: Послання Президента України

2. www.crime-research.ru // Конвенція про кіберзлочинність.

В. А. ЛІПКАН, Ю. Є.МАКСИМЕНКО, В. М. ЖЕЛІХОВСЬКИИ

РОЗДІЛ 9
БЕЗПЕКА ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА ЄВРОПЕЙСЬКОГО СОЮЗУ

У більшості розвинених країн за участю політичних лідерів, прогресивних урядів та фінансової підтримки транснаціональних корпорацій реалізуються Програми становлення інформаційного суспільства; концепції переходу до інформаційної ери, плани участі в трансформації суспільних інститутів, прийняті міжнародними організаціями ООН/ЮНЕСКО, Світовим банком, Світовою Організацією Торгівлі, Організацією економічного співробітництва і розвитку, Радою Європи, Європейським Союзом, Європейським банком реконструкції і розвитку, ОБСЄ, Центральноєвропейською Ініціативою та іншими міжнародними і регіональними урядовими і неурядовими інституціями. За основу Концепцій взято визначення стратегії інформаційного суспільства, основних положень, умов і пріоритетів міжнародної, регіональної і національної інформаційної політики, формулюються політичні, правові, соціально-економічні, культурні і технологічні передумови переходу до інформаційного суспільства, обґрунтовується специфіка і мета глобальних трансформацій.

/. *Основні положення Окінавської Хартії глобального інформаційного суспільства*

Одним з перших концептуальних документів, що визначив стратегію побудови інформаційного суспільства, є прийнятий 29 сесію Генеральної Конференції **ЮНЕСКО у 1996 році** документ під назвою **«Інформаційне суспільство** для всіх».

Ідея інформаційного суспільства, викладена у даному документі, як ідеологія міжнародного розвитку, передбачає осмислення нового етапу існування цивілізації, трансформацію традиційних економічних відносин, зміну соціальних факторів

у життєдіяльності суспільства, нові форми міжкультурної комунікації.

Диференційована політика ЮНЕСКО в європейському регіоні здійснюється на основі відмінностей інформаційного розвитку країн Західної, Центральної та Східної Європи.

Так, взаємодія ЮНЕСКО з Європейським Союзом, передбачає дослідження нових ринків інформаційних продуктів та послуг, передачу нових технологій (ноу-хау), поширення знань з метою сталого розвитку, створення урядових електронних мереж для ефективного управління.

Серед основних європейських нормативно-правових актів, що регулюють суспільні відносини у сфері побудови інформаційного суспільства є **Окінавська хартія глобального інформаційного суспільства від 22 липня 2000 року.** У преамбулі цього міжнародного договору зазначається, що інформаційно-комунікаційні технології (ІТ) є одним з найбільш важливих факторів, що впливають на формування суспільства XXI століття. Вони (ІТ) революційно впливають на життя людей, взаємодію уряду та громадянського суспільства.

Далі в документі зазначається, що інформаційне суспільство дозволяє людям ширше використовувати свій потенціал та реалізовувати свої спрямування. Але для цього необхідно, щоб ІТ забезпечували стійке економічне зростання, збільшення суспільного добробуту, стимулювання соціальної згоди та повної реалізації їх потенціалу в сфері зміцнення демократії, транспа-рентного та відповідального управління, прав людини, розвитку культурного багатоманіття та укріплення міжнародного миру та стабільності.

Для досягнення поставлених цілей та вирішення можливих проблем необхідно розробити ефективні національні та міжнародні стратегії.

У Хартії виокремлюються **наступні загрози становленню глобального інформаційного суспільства:**

1. Міжнародний розрив в галузі інформації та знань (п.5).

2. Інформаційні зловживання, що загрожують цілісності мережі та комп'ютерна злочинність (п.4, п. 8).

3. Загроза захисту авторського права та права на інтелектуальну власність (п.7).

4. Загроза технологічних можливостей окремих регіонів та країн (п.7).

5. Загроза захисту приватного життя споживача взагалі та при обробці даних зокрема (п.7).

6. Загроза безпеці інформаційних систем (п.8).

7. Різниця у володінні інформаційними навичками окремих людей (п.11).

Як зазначається в самій Хартії, вона є закликом до всіх як державних, так і приватних секторів, ліквідувати міжнародний розрив у сфері інформації та знань. Ефективне партнерство серед учасників, включаючи спільне політичне співробітництво, є ключовим елементом раціонального розвитку інформаційного суспільства. Завданням всіх суб'єктів міжнародної спільноти та окремої людини полягає не тільки стимулювання та сприяння переходу до інформаційного суспільства, а також в повній реалізації його економічних, соціальних та культурних переваг (п.6).

Для досягнення цих завдань, а також для управління вищезазначеними загрозами дана Хартія передбачає наступні напрями європейської політики інформаційної безпеки:

1. Проведення економічних та структурних реформ з метою створення обстановки відкритості, ефективності, конкуренції та використання нововведень.

2. Розробка інформаційних мереж, що забезпечують швидкий, надійний, безпечний та економічний доступ за допомогою конкурентних ринкових умов та відповідних нововведень до мережевих технологій, їх обслуговуванню та використанню.

3. Розвиток людських ресурсів, здатних відповідати вимогам століття інформації, шляхом освіти та навчання протягом життя та задоволення попиту на спеціалістів у галузі IT в усіх сферах нашої економіки.

4. Активне використання ІТ в державному секторі реального часу послуг, необхідних для збільшення рівня доступності влади для усіх громадян.

5. Ефективне партнерство між державним та приватним сектором в сфері використання інформаційних технологій.

Слід зазначити, що в Окінавській хартії особливу роль посідає боротьба з комп'ютерною злочинністю як однієї з найнебез-печніших загроз інформаційного суспільства. Так, нормативно закріплено, що зусилля міжнародного співтовариства, спрямовані на розвиток глобального інформаційного суспільства, мають супроводжуватись узгодженими діями зі створення безпечного та вільного від злочинності кіберпростору. Задля чого необхідно віднайти ефективні політичні рішення актуальних проблем, наприклад, спроби несанкціонованого доступу та комп'ютерні віруси, а також залучати представників промисловості та інших посередників для захисту важливих інформаційних інфраструктур. Подальшого розвитку дані положення Хартії знайшли відображення в Європейській Конвенції «Про кіберзлочини» від 23 листопада 2001 року, який був підписаний тридцятьма країнами, серед яких і Україна, з метою вироблення єдиної ефективної позиції протидії кіберзлочинам.

Особливо важливим, акцентується в Хартії, залишається питання подолання електронно-цифрового розриву всередині країни та за її межами. Кожна людина повинна мати можливість доступу до інформаційних й комунікаційних мереж. Стратегія розвитку інформаційного суспільства має супроводжуватись розвитком людських ресурсів, можливості яких відповідали вимогам інформаційного століття. Європейський Союз та окремі країни Європи зобов'язуються надати всім громадянам можливість засвоїти та отримати навички роботи з ІТ шляхом освіти, навчання та підготовки протягом життя.

Значну увагу в даному документі приділяється допомозі становленню інформаційного суспільства та входження до глобального інформаційного простору країнам, що розвиваються.

Зазначається, що держави, які не встигають за високими темпами розвитку ІТ, позбавлені можливостей в повному обсязі брати участь в житті інформаційного суспільства та економіки. Для вирішення цієї проблеми слід ураховувати різноманітність умов та потреб цих країн. Важливу роль при цьому мають відіграти власні ініціативи в прийнятті послідовних національних програм з метою реалізації політичних заходів, направлених на підтримку ІТ та конкуренції в цій сфері, а також створення нормативної бази, використання ІТ в інтересах вирішення завдань у сфері розвитку та в соціальній сфері, розвитку людських ресурсів, що мають навички роботи з ІТ (п. 14).

Довгостроковою *метою* для становлення глобального інформаційного суспільства є подолання міжнародного розриву, що головним чином залежить від ефективного міжнародного двох-стороннього та багатостороннього співробітництва. Велика роль у цих процесах відводиться міжнародним організаціям та установам - банкам розвитку, Міжнародній мережі телекомунікацій та різноманітним міжнародним фондам.

Зазначається, що країни Європи в подальшому сприятимуть зміцненню зв'язків між розвиненими країнами та країнами, що розвиваються, шляхом фінансового, технічного та політичного забезпечення з метою оптимального клімату для використання інформаційних технологій.

Саме для цього пропонується створити «Групу з можливостей інформаційних технологій », завданням якої буде вивчення можливостей держав до входження до глобального інформаційного суспільства, особливо країн, що розвиваються. Після цих досліджень Група пропонуватиме використовувати конкретні заходи у сферах формування політичного, нормативного та мереженого забезпечення, покращення технічної сумісності, розширення доступу та зниження витрат, а також зміцнення людського потенціалу тощо.

Таким чином, Окінавська хартія глобального інформаційного суспільства закликає до розробки єдиної спільної стратегії по-

будови інформаційного суспільства, що призведе до вирішення ряду глобальних проблем та соціально-економічного прогресу всіх держав.

2. Європа і глобальне інформаційне суспільство

Діалектичний взаємозв'язок європейської та глобальної стратегій становлення інформаційного суспільства репрезентований у концептуальній доповіді Європейської Комісії з проблем інформаційного суспільства «Європа і глобальне інформаційне суспільство: рекомендації для Європейської Ради ЄС» у 1994 році.

У даній доповіді зазначається, що глобальні інформаційні процеси впливають на встановлення нової ієрархії держав, відкривають нові можливості промислового розвитку, обумовлюють створення відповідної правової бази, підвищують рівень обміну культурою та традиціями. Європа усвідомлює важливість глобального співробітництва і необхідність правил для інформаційного суспільства, які стосуються права на інтелектуальну власність, недоторканність приватного життя, охорони персональних даних, інформаційної безпеки, використання інформаційного ресурсу, заборони незаконної інформації. Якщо Європа не зможе ефективно адаптуватися до нових умов, вона втратить конкурентоспроможність на світових і регіональних ринках і матиме соціальні проблеми в європейських країнах.

Квінтесенцією даного документу є визначення становища держави в міжнародному середовищі не за географічним розташуванням, кількістю природних ресурсів, кліматичними умовами та соціально-економічним потенціалом, а рівнем впровадження наукових досягнень й високих технологій в усі сфери життєдіяльності суспільства.

Реалізація стратегії інформаційного суспільства в Європейському Союзі базується на досить потужному матеріально-фінансовому забезпеченні. На розвиток ідей інформаційної політики ЄС в окремих сферах життєдіяльності суспільства створюють-

 моделі, криза якої супроводжується прогресуючим демографічним дисбалансом населення. Перед організацією також стоїть дилема: як досягти прискореного економічного зростання і водночас зберегти європейські цінності соціальної солідарності.

Серед основних заходів для вирішення вищезазначених проблем на даному Самміті було ухвалено реалізувати *План дій «е-Еигоре»* на основі документів Європейської Комісії - «Ініціатива e-Europe» та «Стратегія працевлаштування в інформаційному суспільстві».

Даний План передбачає широке впровадження технологій Інтернету для розвитку електронної комерції та інформаційних послуг, а також розвиток знань і навичок населення європейських країн, необхідних для існування в інформаційному суспільстві.

Загалом, на основі здійсненого аналізу вищевикладених норм ряду нормативно-правових актів Євросоюзу, можна виокремити, *основні європейські інтереси в інформаційній сфері,* а саме:

а,) **для людини:**

- охорона персональних даних;
- безпека інформації про приватне життя;
- забезпечення конфіденційності міждержавних інформаційних відносин;

б) для суспільства та Союзу:

- вплив на структуру європейської спільноти і систему цінностей;
- відтік інтелектуальних ресурсів;
- технологічна залежність від США та Японії.

До ***основних напрямів інформаційної політики ЄС*** для управління загрозами з метою реалізації вище зазначених інтересів належать:

1) удосконалення нового суспільного середовища;

2) поглиблення міждержавного співробітництва в умовах становлення інформаційного суспільства;

3) забезпечення вільного обігу інформації в суспільстві для підвищення ступеня демократичної участі країн у політичних процесах;

4) побудова економіки знань (інформаційної економіки);

5) створення та використання конкурентноспроможних ін формаційних ресурсів та потенціалу Європи в міжнародному економічному середовищі;

6) недопущення злочинів у кіберпросторі;

7) забезпечення працевлаштування європейського населення в інформаційному суспільстві;

8) вільний доступ до ресурсів мережі Інтернет;

9) недопущення розшарування суспільства за інформаційною ознакою на «інформаційно багатих» та «інформаційно бідних»;

10) поширення ідей, знань, інформації на рівноправних підставах для всіх народів європейського регіону;

11) використання спільної європейської інформаційної спадщини на благо цивілізації;

12) захист інформаційної інтелектуальної власності;

13) розширення інформаційної інфраструктури в Європі шляхом створення панєвропейської інформаційної магістралі «EuroNet».

Слід зазначити, що в інформаційному суспільстві кожний громадянин країн-членів ЄС має право доступу до даних відкритого характеру (закони, урядові рішення, інформацію засобів масової комунікації), культурної спадщини (літературні твори, не обмежені авторським правом і віднесені до національного надбання, наукові праці, безоплатне програмне забезпечення, непатенто-вані стандарти), а також до інформації відкритого характеру в комп'ютерних мережах і системах, що потребує осмислення відповідальності за здійснення нової політики.

Глобальні процеси впливають на національні та регіональні відносини, і завдання європейської спільноти полягає в узагальненні позитивних і негативних наслідків становлення інформаційного суспільства, трансформації демократичних інститутів,

4. Забезпечити ефективне регулювання змісту інформації, що є в мережі Інтернет.

5. Забезпечити захист персональних даних.

6. Забезпечити правовий статус доменів.

7. Забезпечити вільний доступ до масивів інформації в мережі Інтернет для масового використання (Досвід Франції).

У зв'язку з реорганізацією ЄК у 1996 році було створено Генеральний Директорат ЄС з інформаційного суспільства.

Основними завданнями Генерального Директорату є:

1) формування політики інформаційного суспільства в країнах ЄС;

2) розробка регулятивних та правових документів, необхідних для здійснення інформаційної політики в європейському регіоні;

3) створення програм інформаційного суспільства і встановлення взаємодії між політикою розвитку технологій та політикою регулювання інформаційного суспільства;

4) впровадження нових технологій в інші сфери життєдіяльності європейських спільнот;

5) допомога у реалізації програм ЄС, пов'язаних з інформаційним суспільством, зокрема, за напрямками зовнішньої політики, технологічних досліджень, підприємницької ініціативи, конкуренції, єдиного ринку, освіти, культури.

Проблема забезпечення безпеки інформаційного суспільства Євросоюзу посідає особливе місце серед інших повноважень Генерального Директорату ЄС з інформаційного суспільства.

Як зазначає *Макаренко Є А.,* в рамках повноважень Директорату була прийнята програма заходів щодо збільшення безпеки в Інтернет, в якій підкреслюється можливість розробки загальної структури цифрового підпису та кодування для підвищення рівня безпеки електронної торгівлі в Інтернет, а також важливість стимулювання випуску та розвитку криптографічної продукції. Директорат також ініціював розробку та підготовку документів про телекомунікації і супутниковии зв'язок, конвергенцію

медіаіндустрії, аудіовізуальну політику, регулювання інформаційної діяльності, соціальні аспекти інформаційних суперма-гістралей, проблеми соціальної політики в інформаційному суспільстві, антимонопольні заходи в медіабізнесі.

У лютому 1995 року Єврокомісія заснувала Форум інформаційного суспільства (ФІС), основною метою якого є обговорення загальних проблем у економічній, соціальній, державній, освітній, культурній та технологічній сферах становлення інформаційного суспільства.

Даний Форум є консультативним органом ЄС, який не тільки відслідковує загрози становленню інформаційного суспільства, але й виробляє пропозиції та рекомендації щодо їх подолання та нейтралізації.

Учасниками Форуму є представники національних та державних інститутів / організацій, а також представники різних соціальних, фінансових груп, звичайні користувачі, виробники та постачальники інформаційних технологій як країн-учасниць ЄС, так й громадяни інших держав.

Процедура роботи та прийняття рішень ФІС здійснюється в форматі демократичних дискусій з актуальних проблем становлення інформаційного суспільства в сфері економіки, права та культури, що сприяє виробленню подальшого плану дій міжнародної спільноти, прийняття єдиних інформаційних стандартів та уніфікації норм права, що регулюють суспільні відносини в інформаційній сфері.

Рішення Форуму приймаються у вигляді декларацій, директив Єврокомісії Євросоюзу, реалізація яких є обов'язковою для національних урядів країн-членів, але носить дорадчий характер для інших учасників та представників державних та міжнародних організацій.

У рамках Форуму ведуться дискусії та обговорення в наступних напрямах:

1) інформаційне суспільство і підтримка національних ініціатив;

2) соціальні та демократичні цінності, культура і сфери нових послуг засобів масової інформації;

3) зайнятість, створення робочих місць та політики соціального захисту населення в умовах концентрації комунікації;

4) захист прав споживачів, забезпечення права доступу до інформаційних «благ»;

5) трансформація адміністративної та громадської взаємодії;

6) інформаційна «освіченість» населення Європи.

Діяльність Форуму інформаційного суспільства висвітлюються у щорічних доповідях. Так, у першій щорічній доповіді «Мережі для людей і співтовариств» зазначені такі основні проблеми та загрози становленню інформаційного суспільства у Європі, як втрата конкурентоспроможності та інформаційний дисбаланс європейського населення.

На Форумі інформаційного суспільства, проведеного у 1997 році, було наголошено про актуальність таких проблем як захист персональних даних, інформаційна безпека, інформаційна і комп'ютерна освіченість суспільства, багатокультурність та міжнародне співробітництво в інформаційній сфері.

Особливо важливим є забезпечення виконання зобов'язань, проголошеними відповідними нормативно-правовими актами щодо стратегії становлення інформаційного суспільства країн-учасниць та країн-предентендів ЄС.

З метою досягнення прогресу ці країни мають стимулювати інвестиції, створюючи відповідні інформаційні галузі, включаючи подальший прогрес у лібералізації телекомунікацій; забезпечувати безпеку електронної торгівлі, поширення електронної комерції, створення відповідного національного законодавства; прийняття норм права про діяльність засобів масової комунікації в демократичному суспільстві, нового кодексу професійної етики; створити національні консультативні органи (комітети) з впровадження стратегії інформаційного суспільства; запровадити національну організацію (інституцію) для координації виконання національної програми інформаційного суспільства

і поширення інформації про необхідність нових перспектив розвитку.

Такий орган Євросоюзу як Генеральний Директорат ЄС із освіти та культури розглядає проблеми аудіовізуального піратства, комп'ютерної освіченості суспільства, дистанційної освіти та освіти протягом життя, вільного доступу до глобальної інформації, збереження і переведення на цифрову форму досягнень культурного розвитку народів Європи.

Висновки

Окінавська хартія глобального інформаційного суспільства закликає до розробки єдиної спільної стратегії побудови інформаційного суспільства, що призведе до вирішення ряду глобальних проблем та соціально-економічного прогресу всіх держав.

Глобальні інформаційні процеси впливають на встановлення нової ієрархії держав, відкривають нові можливості промислового розвитку, обумовлюють створення відповідної правової бази, підвищують рівень обміну культурою та традиціями. Європа усвідомлює важливість глобального співробітництва і необхідність правил для інформаційного суспільства, які стосуються права на інтелектуальну власність, недоторканність приватного життя, охорони персональних даних, інформаційної безпеки, використання інформаційного ресурсу, заборони незаконної інформації. У документі підкреслюється, якщо Європа не зможе ефективно адаптуватися до нових умов, вона втратить конкурентоспроможність на світових і регіональних ринках і матиме соціальні проблеми в європейських країнах.

Глобальні процеси впливають на національні та регіональні відносини, і завдання європейської спільноти полягає в узагальненні позитивних і негативних наслідків становлення інформаційного суспільства, трансформації демократичних інституїіВ, охорони основних прав і свобод людини в нових умовах, у захисті плюралізму і незалежності засобів масової комунікації,

збереженні національного розвитку, культурної самобутності та мовного розмаїття країн Європи.

Відтак, Євросоюз має достатньо серйозний досвід у сфері становлення та розвитку інформаційного суспільства, де особливе місце надано питанням забезпечення інформаційної безпеки. Даний позитивний досвід доцільно використовувати і в Україні в контексті реалізації програми становлення інформаційного суспільства (e-Ukraine).

Ключові терміни та поняття *безпека* ***інформаційного суспільства, національні*** *інтереси в сфері становлення* ***інформаційного*** *суспільства, загрози* ***інформаційному суспільству***

Контрольні запитання для самоперевірки

1. Дайте визначення поняття «інформаційне суспільство», яке законодавчо закріплене Євросоюзом.

2. Розкрийте зміст основних міжнародних нормативно-правових актів, що регулюють суспільні відносини у сфері побудови інформаційного суспільства.

3. Як співвідносяться міжнародні нормативно-правові акти та нормативно-правові акти Євросоюзу у сфері становлення інформаційного суспільства?

4. Яке місце у сфері становлення інформаційного суспільства Євросоюзу займають питання «безпеки»?

5. Назвіть структуру органів Євросоюзу, до компетенції яких належать питання становлення інформаційного суспільства.

6. Які заходи передбачає Євросоюз для забезпечення безпеки інформації в мережі Інтернет?

7. Назвіть основні національні інтереси в інформаційній сфері Євросоюзу.

Завдання для самопідготовки

1. Система інформаційного безпеки Євросоюзу.

2. Окресліть механізм взаємоузгодження національних інтересів різних країн Європи в інформаційній сфері.

Список рекомендованої літератури

Доктринальні джерела

1. Basic Documents UNESCO 1989-1995. News Communication Strategy. Document C II-96/WS/2. - Paris, UNESCO, 1995. -109 p.

2. Building the European Information Society for Us All. First Reflections of the High Level Group of Experts. Interim Report. -Brussels, 1996.

3. Convention on Cybercrime. Explanatory Report. Budapest, 23, November, 2001. Council of Europe.

4. Dutton W., Blumler J., Garnham N. et all. The Politics of Information and Commu-nication Policy: The Information Superhighway //Information and Communication Technologies. Visions and Realities. /Ed. by William H. Dutton. - Oxford: Oxford University Press, 1996. -Pp. 112-139.

5. Europe and Global Information Society. Recommendations of the High-Level Group on the Information Society to the Corfu European Council (Bangemann Group). European Commission, 1994.

6. Europe's Way to the Information Society: An Action Plan by the European Commission. - Brussels, 1994.

7. First Annual Report to the European Commission from the information Society Fo.

8. Green Paper. Living and Working in the Information Society: People First. European Comission. - Brussels, 1996.

9. Networks for People and their Communities. Making the Most of the Information Society in European Union. - Brussels, 1996.

10. White Paper on growth, competitiveness and employment - the challenge and ways forward into 21st century // European Commission, Belgium, 1993. - 54 p.

11. White Paper. The Challenges and Ways Forward into the 21st Century. - Brussels, 1993.

12. *Арістоеа LB.* Державна інформаційна політика та її реалізація в діяльності ОВС України: організаційно-правові засади: Дис. д-ра. юрид. наук: 12.00.07 / Націон. ін-т внутр. справ. - Х., 2002.-408 с

13. *Макаренко ЄА.* Європейське інформаційне суспільство: виклики XXI століття для країн Центральної та Східної Євро пи // Вісник Київського університету. Міжнародні відносини. - 2000.-№16. - С 81-87.

14. *Макаренко ЄА.* Міжнародна інформаційна політика: структура, тенденції, перспективи: Дис. д-ра. політич. наук: 23.00.04 / Київ, націон. ун-т ім. Т.Шевченка. - К., 2003. - 475 с

15. Окінавська хартія глобального інформаційного суспільс тва від 22 липня 2000 року.

РОЗДІЛ 10
АДАПТАЦІЯ СТАНДАРТІВ ЄВРОПЕЙСЬКОГО СОЮЗУ УКРАЇНОЮ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Вступ

Політика євроінтеграції є вагомою складовою загальної політики національної безпеки України. Утім, підміна акцентів з адаптації евро стандартів, на адаптацію законодавства України під евро стандарти змушують зосередити увагу на основному змісті цих стандартів, а також формуванню вірного уявлення читача про зміст механізму адаптації і його цільове призначення.

1. Право Європейського Союзу

Вже на початку інтеграційного процесу політичними інституціями ЄС колишні соціалістичні країни було поділено на три групи:

1) держави Центральної, Східної Європи;

2)балканські країни;

3) Росія й інші держави СНД.

До першої групи входили такі країни: Польща, Угорщина, Чехія, Словаччина, Словенія, Болгарія, Румунія, Литва, Латвія та Естонія, співробітництво з якими відбувалось на основі асоційованих Європейських угод.

До другої - Федеративна республіка Югославія (Сербія і Чорногорія), Хорватія, Албанія, Македонія, Боснія і Герцеговина. Після нормалізації ситуації в цих країнах планувалась взаємодія з ЄС в рамках угод про стабілізацію і асоціацію.

До третьої ~ Росія, Україна, Грузія та інші держави СНД, з якими могли бути чи вже були укладені угоди про партнерство та співробітництво.

Характер взаємодії між країнами, що утворились після розпаду Радянського Союзу та ЄС залежав від їх економічного, політичного, соціального потенціалу.

В. А. ЛІПКАН, Ю. Є.МАКСИМЕНКО, В. М. ЖЕЛІХОВСЬКИИ Гнатовськаіі М.М. зазначає, що здебільшого виокремлюють три основні організаційно-правові форми європейської інтеграції - Європейський Союз, Раду Європи та Організацію з безпеки і співробітництва в Європі. Дослідники кожної з головних організаційних форм європейської інтеграції неминуче проходять через спокусу визначити правову систему, яка створена відповідною організацією, «європейським правом».

Як правило, під «європейським правом» розуміється:

- сукупність національних правових систем європейських де ржав, незважаючи на досить суттєві відмінності, зокрема, між англосаксонським загальним правом та романо-германським правом;

~ регіональна чи навіть, субрегіональна міжнародно-правова система;

- сукупність правових норм, які регулюють відносини, що складаються переважно між державами Європейського Союзу.

Така невизначеність у застосуванні терміну «європейське право» може свідчити лише про те, що нині ще не можна стверджувати про існування правової системи, яка повною мірою заслуговує на таку назву, тому не можна погоджуватися з тими з авторів, які ототожнюють поняття «європейське право» та «право Європейського Союзу». Останнє, хоча й декларувалося його творцями як «європейське», проте стати таким воно може лише із розповсюдженням сфери його дії на більшість, а потенційно -на всі держави Європи. Більш того, називати «європейським правом» лише право Європейського Союзу означало б ігнорування права Ради Європи та ОБСЄ, які роблять дуже суттєвий внесок у справу формування спільного для всіх європейських держав.

Як зазначалось раніше, виходячи зі змісту установчих договорів Європейського союзу, він особливу увагу приділяє розвитку спільної політики в таких сферах, як *економічна, з вугілля та сталі та з атомної енергії,* що прямо витікає з установчих договорів (Договір про заснування Європейського об'єднання вугілля та сталі, Договір про заснування Європейського Еконо-

мічного Співтовариства та Європейського Співтовариства з атомної енергії (Євроатом), *зовнішня політика та політика безпеки,* а також *співробітництва поліцій і судів в кримінально-правовій сфері (в галузі юстиції та внутрішніх справ).*

Саме Маастрихтський договір запровадив поняття «трьох опор», кожна з яких тотожна вищезазначеним сферам. Важливість даного нормативно-правового акта підтверджується ще й тим, що вперше було закріплені загальна зовнішня політики та політика безпеки країн ЄС, а саме:

- захищати загальні цінності, основні інтереси та незалежність Союзу;
- зміцнювати безпеку Союзу та держав-членів усіма способами;
- підтримувати мир та зміцнювати міжнародну безпеку згідно з принципами Статуту ООН, Гельсінського заключного акта та цілями Паризької хартії;
- сприяти міжнародному співробітництву;
- розвивати та консолідувати демократію й законність, пова гу до прав людини й основних свобод.

Одразу зазначимо, що право Європейських Співтовариств є складовою права Європейського Союзу.

Аналіз науково-практичних та нормативно-правових джерел дозволяє виокремити ряд специфічних *характерних ознак праву* Європейського Союзу щодо права держав-учасниць.

1. Інтернаціоналізація національних правових систем шляхом рецепції, апроксимації (зближення). Основними формами зближення є гармонізація (повна, часткова, альтернативна, мінімальна) та уніфікація.

2. Процес зближення законодавств держав-членів ЄС є багатоетапним. На першому етапі органи ЄС встановлюють певні правила (засади, стандарти) усунення протиріч у національних законодавствах країн-учасниць у відповідних напрямках правового регулювання, які в подальшому імплементуються. На другому етапі, до їх національного права з урахуванням спе-

 цифіки механізму прийняття певних змін до правової системи цих держав (процес гармонізації). Але, процес гармонізації має ряд винятків у випадках, передбачених статтею 36 Римського договору (міркування суспільної моралі, суспільного порядку та державної безпеки, захисту здоров'я і життя людей та/або тварин, збереження рослин, захисту національних скарбів, що мають художню, історичну чи археологічну цінність, захисту промислової і торговельної власності), чи пов'язаних із захистом умов праці або навколишнього середовища, внаслідок чого будь-яка країна-учасниця може визнати за необхідне застосування власних національних норм права щодо права ЄС. Дані питання, вирішуються виключно в судовому порядку.

Процес уніфікації відбувається на підставі окремих договорів (угод), що потребує обов'язкової згоди кожної країни-учасниці ЄС в чітко закріплених сферах, наприклад, забезпечення застосування та захисту прав своїх громадян на тих же умовах, що надаються кожною державою власним громадянам; усунення подвійного оподаткування в Співтоваристві; взаємне визнання компаній та збереження їх правосуб'єктності при перенесенні місцезнаходження компаній з однієї країни до іншої, а також забезпечення можливості злиття компаній, що керуються законами різних країн; спрощення взаємного визнання та виконання судових та арбітражних рішень.

Угода про партнерство та співробітництво між Європейськими Співтовариствами, їх державами-членами та Україною закріпила необхідність гармонізації законодавства України із правом Європейського Союзу.

Крім того, як зазначає *Мураейое В.І.,* Україна, не будучи членом ЄС, може приймати нормативно-правові акти, що відповідають праву ЄС, здійснюючи у такий спосіб непряму гармонізацію.

1. Право ЄС має пріоритетний та доповнювальний характер щодо національних правових систем держав-учасниць.

2. Відповідно до ст. 189 Договору про створення ЄЕС норми права ЄС є нормами прямої дії на території держав-учасниць. Суд Європейських Співтовариств вказав на те, що самі держави-учасниці ЄС, створивши на невизначений час Співтовариство, що має свою власну організаційну структуру, власні право- і дієздатність, право виступати на міжнародній арені в якості самостійної юридичної особи, обмежили свої суверенні права (хоча й у рамках лише деяких сфер) і створили систему права, обов'язкову як для них самих, так і для їхніх юридичних і фізичних осіб.

3. Принцип верховенства права ЄС над національним правом держав-учасниць розглядається в якості неписаного (через відсутність його закріплення в якому-небудь з установчих договорів про створення ЄС), але, разом з тим, основного правила, що діє в рамках ЄС, крім того, застосування даного принципу не залежить від того, коли прийнята та чи інша норма внутрішнього національного права: до чи після вступу в силу норми права ЄС, що їй не відповідає. В усіх випадках пріоритет залишається за останньою.

2. Співробітництво України та ЄС у сфері гармонізації інформаційного законодавства

Розвал Радянського Союзу призвів до появи на міжнародній арені нових незалежних країн, зокрема й України. Одразу після проголошення Незалежності Україною 2 грудня 1991 року Євро-союз прийняв Декларацію Європейського Співтовариства щодо України, визнаючи, таким чином, її суверенітет.

Більш того, Директива Європейського Співтовариства щодо визнання нових держав у Східній Європі та Радянському Союзі від 16 грудня 1991 р. зазначила про готовність Співтовариства і держав-членів визнати ті нові держави, які утворилися на демократичній основі, прийняли відповідні міжнародні зобов'язання

В. А. ЛІПКАН, Ю. Є.МАКСИМЕНКО, В. М. ЖЕЛІХОВСЬКИИ та добросовісно зобов'язалися дотримуватися миру та вести переговори.

Угоду про торгівлю та співробітництво між Радянським Союзом і СЕС та Євроатомом, укладену 18 грудня 1989 р. замінили Угоди про партнерство і співробітництво (УПС), що укладаються між новою незалежною державою з одного боку та Європейськими Співтовариствами і їх державами-членами - з іншого. Дана Угода між Україною та Європейськими Співтовариствами була підписана 14 червня 1994 року та ратифікована Законом України 10 листопада 1994 року. Наразі, тотожні Угоди укладені майже з усіма державами, які утворились унаслідок розпаду СРСР.

Як зазначає український законодавець, у схвалених 2 липня 1993 р. Верховною Радою Основних напрямах зовнішньої політики України, укладання з Європейськими Співтовариствами Угоди про партнерство та співробітництво (УПС) стане першим етапом просування України до асоційованого, а згодом - до повного членства у цій організації.

У ст. 51 даної Угоди зазначається, що сторони визнають важливою умовою для зміцнення зв'язків між Україною та Співтовариством зближення існуючого та майбутнього законодавства України з законодавством Співтовариства. Україна вживатиме заходів для забезпечення того, щоб її законодавство поступово було приведене у відповідність до законодавства Співтовариства.

Важливою є норма даної Угоди, відповідно до якої Співтовариство зобов'язується надати Україні належну технічну допомогу з метою здійснення вищезазначених заходів, яка може включати, зокрема:

- обмін експертами;
- завчасне надання інформації, особливо стосовно відповідного законодавства;
- організацію семінарів;
- професійну підготовку;
- допомогу у здійсненні перекладу законодавства Співтовариства у відповідних секторах (п.3. ст.51).

Логічним продовженням даного пункту Угоди стало підписання 4 липня 2002 року Угоди між Україною та Європейським Співтовариством про наукове і технологічне співробітництво, згідно з якою основними напрямками співробітництва серед інших є технології інформаційного суспільства, науково-технологічна політика.

Необхідно також підкреслити, що згідно з цією Угодою передбачено створення відповідного інституційного механізму, а саме Ради Співробітництва, яка складається з членів Ради Європейського союзу та з членів Комісії ЄС, з одного боку, та членів уряду нових незалежних держав, з іншого, Комітету з питань співробітництва, який складається з представників членів Ради Європейського союзу і членів Комісії європейських співтовариств з одного боку, та з представників уряду нових незалежних держав з іншого, як правило, на рівні старших посадових осіб державної служби, Комітету з парламентського співробітництва, що є форумом, на якому зустрічаються члени Європарламенту та парламенту нових незалежних держав, практичний досвід роботи в яких вже має Україна.

Способи імплементації положень УПС новими незалежними державами можуть полягати в:

1) укладенні двосторонніх договорів з державами-членами ЄС з відповідних питань;

2) прийнятті внутрішніх нормативних правових актів у відповідності з *acquis;*

3) приєднанні до багатосторонніх договорів.

Після того, як Угода про партнерство та співробітництво між Україною і Європейськими співтовариствами та їх державами-членами від 14 червня 1994 р. стала частиною внутрішнього законодавства, Указом Президента України 11 червня 1998 р. було затверджено Стратегію інтеграції України до Європейського Союзу, де, зокрема, йдеться про необхідність чіткого та всебічного визначення зовнішньополітичної стратегії щодо інтеграції України до європейського політичного (в тому числі у сфері зов-

 нішньої політики та політики безпеки), інформаційного, економічного та правового простору.

На основі цієї Стратегії були схвалені Програма інтеграції України до Європейського Союзу від 14 вересня 2000 року, Концепція Загальнодержавної програми адаптації законодавства України до ЄС, Загальнодержавна програма адаптації законодавства України до законодавства ЄС. Указом Президента України від ЗО серпня 2000 р. з метою координації діяльності органів державної влади створено Національну раду з питань адаптації законодавства України до законодавства ЄС, а також на виконання Указу Президента України від 9 лютого **1999** р. «Про заходи щодо вдосконалення нормотворчої діяльності органів виконавчої влади» Кабінет Міністрів запровадив єдину систему планування, координації та контролю роботи з адаптації законодавства.

Одразу зазначимо, що подібна активність притаманна не тільки українській стороні. Зацікавленість ЄС щодо України представлена рядом документів, серед яких чільне місце займає Спільна стратегія ЄС щодо України від 11 грудня **1999** року.

На Копенгагенському саміті ЄС - Україна 4 липня'2002 р. було підтверджено готовність продовжувати співробітництво у пріоритетних сферах і надати динамізму процесові зближення, що об'єктивно сприяє створенню внутрішніх передумов набуття Україною членства в Європейському Союзі.

3. Зміст acquis communautaire

Прагнення України стати членом ЄС обумовило необхідність обов'язкового прийняття ***acquis communautaire*** - сукупності цілей, принципів і норм спільної політики та законодавства ЄС, а також юридичних та інституційних механізмів їхнього впровадження.

На момент свого виникнення *acquis communautaire* включав: - основоположні міжнародні договори, якими засновані Європейські Співтовариства;

- інституційну структуру Співтовариств;
- законодавство Співтовариств;
- міжнародні договори, укладені Співтовариствами;
- акти, прийняті країнами-кандидатами в процесі приєднання до ЄС;
- довгострокові принципи-цілі, які перебувають у процесі визначення;
- обов'язок нового члена безумовно визнати такі основоположні принципи права Європейських Співтовариств, як пряма дія, примат права Співтовариств над національним правом їх членів, а також однакове тлумачення права Співтовариств всіма їх членами.

Стандарти ЄС вважають еталонними. Хоча, як свідчить історичний досвід, існували моменти, коли стандарти ЄС не відповідали, були нижчими за стандарти країн, що мали стати членами ЄС. Наприклад, високі екологічні стандарти Австрії, Швеції і Фінляндії. Внаслідок чого ЄС розробив цілеспрямовану, послідовну сукупність заходів щодо підвищення існуючих стандартів членів ЄС до стандартів країн, що мали стати членами Євросоюзу.

Звідси природним є наявність проблем різного характеру, які можуть виникати у процесі приєднання до *acquis.*

Прикладом, *Гнатовський М.М.* виділяє ряд правових проблем, що ускладнюють прийняття *acquis* країнами Центральної та Східної Європи.

1. Складність структури *acquis* навіть у частині, безпосередньо закладеній основоположними міжнародними договорами, так званому «первинному європейському праві», про що свідчить неузгодженість в фундаментальних, базових поняттях, як от «Європейський Союз» та «Європейські Співтовариства» (досі не зрозуміло, чи включає «Європейський Союз» в себе Європейські Співтовариства та чи має він самостійний юридичний статус), «Рада Міністрів» чи «Рада *Європейського Союзу»,* «асоційоване членство в ЄС» чи «асоційовані відносини» тощо.

2. Велика кількість норм первинного права ЄС застаріла та втратила чинність, а також чинні норми первинного права ЄС треба тлумачити у зв'язку з рішеннями Суду ЄС, які надали цим нормам значення, що безпосередньо не випливає з тексту основоположних договорів.

3. Передумовою імплементації *acquis* є реформа національного конституційного права з метою прийняття примату європейського права та визнання верховної юрисдикції Європейського Суду, отже, існує необхідність проведення конституційної реформи в країнах-кандидатах у зв'язку з наявністю в їхніх конституціях норм, що не дають можливості безумовно прийняти примат європейського права та повною мірою імплементувати *acquis.*

4. Важливі галузі *acquis* постійно перебувають у процесі змін, а отже Комісія ЄС має об'єктивні складнощі в організації процесу спостереження за їх дотриманням у країнах Центральної та Східної Європи, принаймні доки *acquis* у певних сферах не набуде відносної сталості.

5. Розширення на Схід обумовлює значні зміни в інституцій-ній структурі та процедурах прийняття рішень всередині ЄС, що фактично може відбутися тільки разом з внутрішньою реформою Співтовариств.

У зв'язку з вищевикладеними проблемами, ЄС чітко виокремив сфери правового регулювання, де необхідна імплементація норм ЄС країнами кандидатами на вступ.

Особливістю сучасного етапу розширення Євросоюзу є включення до *acquis communautaire* розділу з питань спільної зовнішньої політики і політики безпеки. А тому узгодження політики інформаційної безпеки України з ЄС в цьому напрямку є досить актуальними.

Слід наголосити, що серед багатьох інших сфер, які потребують узгодження з правом ЄС (сфера оподаткування, державних поставок та банківської діяльності, охорони довкілля, енергетики, сільського господарства, промисловості, транспорту, юстиції

та внутрішніх справ тощо) відзначена й сфера інтелектуальної власності та телекомунікацій.

Взагалі, процес вступу країни-кандидата до ЄС складається з ряду послідовних, довготривалих та взаємопов'язаних стадій:

- подання державою до Ради Європейського Союзу заяви щодо членства;
- звернення Ради до Європейської Комісії з проханням підготувати Висновок щодо заяви;
- вручення Висновку Комісією Раді;
- рішення Ради (одностайне) щодо початку переговорів про вступ;
- початок переговорів між державами членами і державою-заявником;
- ухвалення Радою (одностайне) за пропозицією Комісії спільної позиції на переговорах з державою-кандидатом на вступ;
- укладання окремої угоди між Євросоюзом і державою, що вступає, стосовно проекту договору про вступ;
- подання договору про вступ до Ради і до Європарламенту;
- підготовка Комісією висновку щодо договору про вступ;
- надання згоди (абсолютною більшістю) Європарламентом;
- схвалення договору Радою ЄС (одностайне);
- укладення договору між Євросоюзом і країною, що вступає;
- ратифікація договору сторонами;
- набуття договором чинності з визначеної сторонами дати.

Зазначимо, що в Брюсселі існує думка про безперспективність намагань України стати кандидатом на вступ до Євросо-юзу навіть у віддаленому майбутньому, але українські вчені вважають, що необхідно сформувати проукраїнське лобі за допомогою сусідніх країн-членів ЄС, зокрема дружньої до України Польщі.

Вступ до Європейського Союзу не має бути самоціллю. Україна є самодостатньою державою, і її вихід на світової ринки праці та капіталу відбудеться і без Євросоюзу, якщо наша краї-

 на матиме конкурентоспроможну економіку та високі інформаційні технології, які стануть взірцем і стандартом для країн Європи.

Україна має використовувати позитивний досвід Євросоюзу, імплементувати ті положення його законодавства, які сприяють ефективнішому регулюванню суспільних відносин в інформаційній сфері. Сліпе ж копіювання євростандартів, або безальтернативна згода з політикою Європи, нехай і такою, що добре себе зарекомендувала, є таким, що не відповідає національним інтересам. Входження до європейських структур має розглядатися як інструмент реалізації національних інтересів. Ми не маємо прагнути вступати туди, де нас не бажають бачити, де нас просто не чекають. А не чекають тому, що знають потенціал і могутність нашої країни, її омріяну мету щодо становлення центром європейської політики. Не є логічним, коли метою для певної держави є стандарти іншою держави. Але, розглянемо більш детально підходи української влади до адаптації законодавства України до європейських стандартів.

4. Адаптація законодавства України до європейських стандартів: інституційний підхід

У Посланні Президента України до Верховної Ради України «Європейський вибір. Концептуальні засади стратегії економічного та соціального розвитку України на 2002 - 2011 роки» заплановано протягом 2002-2007 рр. приведення законодавства України у відповідність до вимог законодавства ЄС у пріоритетних сферах.

Розуміючи, що приведення українського законодавства у відповідність до європейських стандартів неможливе без відповідного інституціиного механізму, на базі Центру європейського та порівняльного права, відповідно до Постанови КМУ від 24 грудня 2004 року, був створений Державний департамент адаптації законодавства. Основними завданнями якого є.

1. Організація роботи з реалізації державної політики у сфері адаптації законодавства України до законодавства Європейсько го Союзу.

2. Участь у межах своєї компетенції в координації роботи, пов'язаної з виконанням Загальнодержавної програми адаптації законодавства України до законодавства ЄС.

3. Організація науково-експертного, аналітичного, інформаційного та методологічного забезпечення євроінтеграції.

4. Підготовка рекомендацій щодо приведення законодавства України у відповідність з *acquis communautaire* та на їх підставі розроблення проектів нормативно-правових актів.

5. Проведення експертизи щодо відповідності проектів законів України та інших нормативно-правових актів, що за предметом правового регулювання належать до сфер, правовідносини в яких регулюються правом Європейського Союзу, *acquis communautaire.*

6. Узагальнення інформації про стан адаптації законодавства України до законодавства ЄС.

7. Організація моніторингу імплементації актів законодавства України, проекти яких розроблені відповідно до *acquis communautaire.*

8. Координація в межах своїх повноважень співробітництва між Україною та ЄС у сфері адаптації законодавства України до законодавства ЄС та у сфері юстиції і внутрішніх справ.

Досить важливою функцією даного Департаменту є організація процесу перекладу актів *acquis communautaire* українською мовою та надання їм статусу офіційного.

Переклад відповідних актів здійснюється на основі щорічного орієнтованого плану, який готується Департаментом на підставі пропозицій, що подані центральними органами виконавчої влади та структурними підрозділами Департаменту. Механізм здійснення цього процесу регулюється наказом № 56/5 Міністерства юстиції України «Про затвердження Порядку перекладу актів acquis communautaire на українську мову» від 08.06.2005.

 Процес перекладу акта *acquis communautaire* українською мовою здійснюється в декілька етапів.

1. Переклад повного тексту акта англійською чи французькою мовою з урахуванням всіх чинних змін на початку роботи з його перекладом.

2. Здійснення термінологічної експертизи та літературного редагування переведеного акта.

3. Аналіз відредагованого перекладу Комісією з надання перекладам статусу офіційного щодо отримання цього статусу.

4. Оприлюднення перекладу на Інтернет-сторінці Департаменту протягом 10 робочих днів та ознайомлення центрального органу виконавчої влади, що вносив пропозиції щодо здійснення перекладу такого акта.

Слід зазначити, що термінологічну експертизу та надання статусу офіційних перекладам, може бути здійсненим центральними органами виконавчої влади або іншими установами та організаціями в окремих випадках, передбачених законодавством України.

Динамічність розвитку правових норм ЄС вимагала визначити пріоритетність сфер правового регулювання та, як наслідок, існування відповідного переліку нормативно-правових актів, які в першу чергу повинні бути прийняті країною-кандидатом на вступ,

З аналізу практики можна резюмувати, що більш тривалим є узгодження нормативних актів держав-кандидатів, що регулювали розвиток телекомунікацій та інформаційних технологій, через інтенсивність зміни змісту цього розділу *acquis communautaire* усередині самого Євросоюзу.

Вважаємо важливими пропозиції *АрістовоїІ.В.,* яка зазначила, що розвиток нормативно-правової бази в галузі інформаційної безпеки слід основувати на трьох головних принципах. По-перше, проекти нормативно-правових актів, що розробляються, повинні бути максимально «технологічно нейтральними», щоб будь-яка, незначна інновація не призводила до необхідності

терміново вносити зміни у законодавство. Відомо, наскільки далеко від цього українське інформаційне законодавство. По-друге, слід уникати надмірного регулювання. У ряді випадків розвиток саморегулювання, дотримання етичних і моральних норм на основі «корпоративного» права може бути більш ефективним засобом створення цивілізованого правового простору. І, нарешті, оскільки інформаційна сфера є найбільш чутлива до різниць у правових нормах, що регулюють створення та використання інформаційних мережевих технологій у різних країнах, необхідно забезпечити гармонізацію законодавства на міжнародному рівні.

Висновки

Зазначимо, якщо навіть будь-яка з колишніх радянських республік, що географічно розташована в Європі, і відповідатиме усім критеріям до вступу і ЄС не матиме ґрунтовних причин для відмови, інтеграційний процес все одно лишатиметься політичним процесом, який умисно оформлюють різними критеріями для виконання. Насправді ж, потрібно чітко усвідомлювати: мало хто бажає бачити Україну в Європейському Союзі. Вочевидь, Україна може опинитися там лише тоді, коли сама об'єктивно сформує інформаційне суспільство, процвітаючу економіку, могутню систему безпеки. За інших умов, постійне прагнення щодо відповідності нашої держави певним критеріям перетворить функціонування України на постійне прагнення відповідності чомусь, а коли ми досягнемо того до чого прагнули, будуть сформовані нові критерії та вимоги, формування постінформаційного суспільства. Відтак замість блукання манівцями відповідності євростандартів, Україна має узяти найкращі взірці як законодавства, так і практики його застосування на озброєння та крокувати власним шляхом побудови процвітаючого демократичного суспільства і побудови могутньої держави.

 Саме тому українська сторона має досить активно співпрацювати з Євросоюзом з метою формування ефективного механізму реалізації національних інтересів. Адаптація має стосуватися не українського законодавства, а стандартів Європи до формування підвалин для стійкого розвитку України. Не ми маємо пристосовуватися до когось, а маємо узяти краще для побудови свого найкращого.

Ключові терміни та поняття

acquis communautaire, європейське право, інтеграція, адаптація, право Європейського Союзу

Контрольні запитання для самоперевірки

1. Дайте визначення поняття «європейське право».
2. Як співвідносяться поняття «право Європейських Співтовариств» та «право Євросоюзу».
3. Назвіть основні ознаки права Євросоюзу.
4. Охарактеризуйте Угоду між Україною та Європейськими Співтовариствами, яка була підписана 14 червня 1994 року.
5. Назвіть основні правові проблеми, що ускладнюють прийняття acquis країнами Центральної та Східної Європи.
6. Розкрийте основні етапи процесу вступу країни-кандидата доЄС.
7. Охарактеризуйте діяльність основних органів України в сфері адаптації українського законодавства *до права Євросоюзу.*

Завдання для самопідготовки

1. У чому полягає різниця між адаптацією законодавства і адаптацією європейських стандартів?
2. Окресліть механізм маніпуляції термінологією на прикладі: входження до евро атлантичних структур як національний інтерес і формування могутньої системи безпеки (через співпрацю з євроатлантичними структурами) як національний інтерес.

Список рекомендованої літератури

Нормативні джерела

1. Конституція України // Відомості Верховної Ради (ВВР). -1996. - №30.-Ст. 141.
2. Договор об Европейском союзе 1992 г. - Страсбург, 1992 -С 19.
3. Європейський вибір. Концептуальні засади стратегії еко номічного та соціального розвитку України на 2002-2011 роки: Послання Президента України до Верховної Ради // Урядовий кур'єр. - 2002. - 4 червня.
4. Про Загальнодержавної програми адаптації законодавства України до законодавства Європейського Союзу Закон України від 18 березня 2004 року.
5. Про затвердження Стратегії інтеграції України до Європейського Союзу: Указ Президента України від 11 червня 1998 року.
6. Про Концепцію Загальнодержавної програми адаптації законодавства України до законодавства Європейського Союзу: Закон України від 21 листопада 2002 року.
7. Про Національну раду з питань адаптації законодавства України до законодавства Європейського Союзу Указ Президента України від 30 серпня 2000 року.
8. Програма інтеграції України до Європейського Союзу: Указ Президента України від 14 вересня 2000 року.
9. Угода про партнерство та співробітництво між Україною і Європейськими співтовариствами та їх державами-членами, підписана 14 червня 1994 р. в Люксембурзі, ратифікована Зако ном України від 10 листопада 1994 року.

Доктринальні джерела

1. Agenda 2000: For A Stronger And Wider Union. - Strasbourg, 15 July 1997. - DOC/97/6.

2. Avery G., Cameron F. The Enlargement of the European Union. - Sheffield: Sheffield Academic Press, 1998. - 199 p.

3. Balazs P. The EU's Collective Regional Approach to its Eastern Enlargement: Consequences and Risks. - Copenhagen: Copenhagen Research Project on European Integration, 1997. - 38 p.

4. Building the European Information society for us all: Final policy report of the high - level expert group, April 1997 // European Commission. Directorate - General for employment, industrial relation and social affairs. Unit V/B/4. - Brussels, manuscript completed in April 1997. - 77 p.

5. Common Foreign and Security Policy and Enlargement. -Gütersloh: Bertelsmann Foundation Publishers, 1995. - 117 p.

6. Craig P., de B-brc6G. EC Law: Text, Cases, Materials. -Oxford: Clarendon Press, 1997. - CXXXVI p. + 1160 p.

7. EC Guidelines On The Recognition of New States in Eastern Europe and in the Soviet Union // Basic Documents Supplement to International Law Cases and Materials / Louis Henkin et al. -St.Paul.,1993.-P. 62.

8. Gialdino C. Some Reflections on the Acquis communautaire // Common Market Law Report. - 1995. - No. 32. - P. 1089-1121.

9. Goebel R. J. The European Union grows: the constitutional impact of the accession of Austria, Finland and Sweden // Fordham International Law Journal, No. 18(4), 1995. -P. 1140-1149.

10. Slot P.J. Harmonization // European Law Review. - 1996. -№2.- P.379-389.

11. White Paper on growth, competitiveness and employment -the challenge and ways forward into 21st century // European Commission, Belgium, 1993. - 54 p.

12. *Арістоеа LB.* Державна інформаційна політика та її реалізація в діяльності ОВС України: організаційно-правові засади: Дис. д-ра. юрид. наук: 12.00.07/ Націон. ін-т внутр. справ. - Х., 2002.-408 с

13. *Барановский В.Г.* Европейское сообщество в системе международных отношений. - М.: Мысль, 1986. - С.270.

14. *Брыжко В. М., Орехов АЛ., Гальченко О.Н.* и др. К Пуду щее информационное право. - К.: Интеграл, 2002. - 264 с.

15. *Гнатовський М.М.* Становлении га тенденції розвитку європейського правового простору: Дис. ... канд.. юрид. наук: 12.00.11 / Київ. нац. Ун. 1м.. Т. Шевченка. К., 2002. - 193 с.

16. Европейское право. Учебник для вузов / Под общ. ред. Л.М. Энтина. - М.: Норма, 2000. - 720 с.

17. *Ковальова О.О.* Українська політика щодо євроінтегра-ційних процесів: Дис. ... д.-ра політич. наук: 23.00.02 / Націон. акад.. наук Укр., Ін-т політ, та етнонац. процесів. - К., 2003. -369 с.

18. *Макаренко ЄА.* Міжнародна інформаційна політика: структура, тенденції, перспективи: Дис. д-ра. політич. наук: 23.00.04\ Київ, націон. ун-т ім. Т.Шевченка. - К., 2003. - 475 с

19. *Муравйов В.І.* Способи зближення законодавства України та права Європейського Союзу // Проблеми гармонізації законодавства України з міжнародним правом. - К., 1998. - С. 138-140.

20. Оцінка Електронної готовності України /Стратегічні реко-мендації/ Доповідь у рамках проекту Уряду України / ПРООН - «Інноваційний трамплін: ІКТ задля добробуту України». - К.: Держ. ком. зв'язку та інформатизації України, - 2002 .-8с.

21. *Снігир О.В.* Україна в геополітичних концепціях Європейського Союзу: динаміка «Об'єкт - суб'єктних» відносин: Дис. ... канд. політич. наук: 21.01.01 / Націон. ін.- т стратегіч. досліджень. - К., 2004. - 178 с

В. А. ЛІПКАН, Ю. Є.МАКСИМЕНКО, В. М. ЖЕЛІХОВСЬКИИ

ТЕЗАУРУС

ACQUIS COMMUNAUTAIRE - сукупність цілей, принципів і норм спільної політики та законодавства ЄС, а також юридичних та інституцій-них механізмів їхнього впровадження. На момент свого виникнення *acquis communautaire* включав: основоположні міжнародні договори, якими засновані Європейські Співтовариства; інституційну структуру Співтовариств; законодавство Співтовариств; міжнародні договори, укладені Співтовариствами; акти, прийняті країнами-кандидатами в процесі приєднання до ЄС; довгострокові принципи-цілі, які перебувають у процесі визначення; обов'язок нового члена безумовно визнати такі основоположні принципи права Європейських Співтовариств, як пряма дія, примат права Співтовариств над національним правом їх членів, а також однакове тлумачення права Співтовариств всіма їх членами.

АБСОЛЮТНА БЕЗПЕКА — 1) свідомий цілеспрямований вплив на загрози та небезпеки, за якого створені умови для безперешкодної реалізації усієї гами інтересів об'єкта та повністю виключена можливість дестабілізації його стійкого розвитку; 2) внутрішньо визначена напруженість свободи; 3) стан, за якого ніхто і ніщо нікому не загрожує (філ. роз.).

АБСОЛЮТНА ВІДКРИТІСТЬ — стан системи, в якому зовнішній вплив на будь-який з її елементів перевищує внутрішній.

АБСОЛЮТНА ЗАМКНЕНІСТЬ - стан системи, в якому внутрішній вплив на будь-який з її елементів перевищує зовнішній.

АБСОЛЮТНА СИСТЕМА ЗАХИСТУ - система, в якій наявні усі можливі способи захисту, і яка здатна у будь-який момент свого існування прогнозувати настання загрожуючої події за час, достатній для приведення в дію адекватних способів захисту.

АБСОЛЮТНА СИСТЕМА ЗНИЩЕННЯ - комплекс взаємопов'язаних засобів, здатних будь-яку систему зр :3гти хоча б на деякий час абсолютно відкритою.

АБСОЛЮТНО ВПОРЯДКОВАНА СИСТЕМА - структура, кожний елемент якої має з елементами системи мінімально можливе, але більше від нуля кількість зв'язків. У реальності кількість зв'язків в абсолютно впорядкованій системі не повинна перевищувати 1.

АДАПТАЦІЯ - процес приведення чогось у відповідність до взірця (еталона).

БЕЗПЕКА ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА - свідомий цілеспрямований вплив на загрози та небезпеки, за якого державними, недержавними,

міжнародними або наддержавними інституціями створюються сприятливі умови для функціонування та розвитку *інформаційного суспільства.*

ВИКОРИСТАННЯ ІНФОРМАЦІЇ — задоволення інформаційних потреб громадян, юридичних осіб і держави.

ДЕРЖАВНА ІНФОРМАЦІЙНА ПОЛІТИКА - розуміння діяльності державних органів, спрямоване на врегулювання та розвиток національного інформаційного середовища, що охоплює не тільки телекомунікації, інформаційні системи та засоби масової інформації, а й усю сукупність виробництв і відносин, пов'язаних із створенням, збереженням, обробкою, демонстрацією, передачею інформації у всіх її видах *(визначення Белякова К.І).*

ЄВРОПЕЙСЬКЕ ПРАВО - сукупність національних правових систем європейських держав, незважаючи на досить суттєві відмінності, зокрема між англосаксонським загальним правом та романо-германським правом; регіональна чи то навіть субрегіональна міжнародно-правова система; сукупність правових норм, які регулюють відносини, що складаються переважно між державами Європейського Союзу.

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ - система теоретико-методоло-гічних, нормативно-правових, інформаційно-аналітичних, управлінських, розвідувальних, контррозвідувальних, оперативно-розшукових, кадрових, науково-технічних, ресурсних та інших заходів, спрямованих на забезпечення свідомого цілеспрямованого впливу суб'єкта управління на загрози та небезпеки, за якого державними, міжнародними та недержавними інституціями створюються необхідні й достатні умови для реалізації і прогресивного розвитку інформаційних інтересів, ефективне функціонування самої *системи забезпечення інформаційної безпеки.*

ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ — розмаїття внутрішніх і зовнішніх, об'єктивних і суб'єктивних суперечностей суспільного розвитку в країні й на міжнародній арені в інформаційній сфері, які ускладнюють або унеможливлюють створення сприятливих умов для реалізації національних інтересів в інформаційній сфері, створюють небезпеку для системи інформаційної безпеки, життєзабезпечення її системостворю-ючих елементів

ЗАГРОЗИ ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВУ - розмаїття внутрішніх і зовнішніх, об'єктивних і суб'єктивних суперечностей розвитку інформаційного суспільства, які ускладнюють або унеможливлюють створення сприятливих умов для реалізації його інтересів і створюють небезпеку

для його системи безпеки, життєзабезпечення її системостворюючих елементів

ЗБЕРІГАННЯ ІНФОРМАЦІЇ - забезпечення належного стану інформації та її матеріальних носіїв.

ІНТЕГРАЦІЯ - об'єднання в ціле яких-небудь частин чи елементів.

ІНТЕГРАЦІЯ ІНФОРМАЦІЙНА - 1) різноманітні форми об'єднання декількох просторово-інформаційних секторів. Інтеграція може здійснюватися як внаслідок інформаційної боротьби, так і мирним шляхом. Мета інтеграції - збільшення стратегічного і просторово-інформаційного обсягу блоку; 2) процес поєднання суспільства, держави, міждержавних відносин, на основі загальновизнаних інформаційних цінностей, національних інформаційних інтересів; характеризується великим обсягом і високою інтенсивністю інформаційних взаємозв'язків і взаємодій.

ІНФОРМАЦІЙНА АГРЕСІЯ - незаконні дії однієї зі сторін в інформаційній сфері, спрямовані на нанесення супротивнику конкретного, відчутного збитку в окремих областях його діяльності шляхом обмеженого і локального по своїх масштабах застосування сили. Ознаки інформаційної агресії: виключення із засобів інформаційної дії самих небезпечних видів, що не дозволяють надійно контролювати розміри завдається збитку - інформаційної зброї; обмеження розмірів простору, об'єктів інформаційної інфраструктури і соціальних груп, що піддаються ураженню інформаційною дією (агресія зачіпає не весь інформаційний простір держави-жертви, а тільки його частина); обмеження по меті (переслідує локальну, приватну мету) і часу (як правило, агресія припиняється після повного досягнення агресором всієї поставленої конкретної мети і рідко приймає затяжний характер), а також по силах і засобах, що залучається.

ІНФОРМАЦІЙНА БЕЗПЕКА - складова національної безпеки, свідомий цілеспрямований вплив суб'єкта управління на загрози та небезпеки, за якого державними та недержавними інституціями створюються необхідні та достатні умови для; забезпечення інформаційного суверенітету України; вдосконалення державного регулювання розвитку інформаційної сфери, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активного залучення засобів масової інформації до боротьби з корупцією, зловживанням службовим становищем, іншими явищами, які загрожують національній безпеці України, неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяль-

ність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції; вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

ІНФОРМАЦІЙНА БЕЗПЕКА ЄВРОПЕЙСЬКОГО Союзу — захист особистої інформації про відправників і одержувачів, захист інформації від несанкціонованих змін, захист від несанкціонованого доступу до інформації і створення надійного джерела постачання обладнання, послуг та інформації. І.б.Є.с також охоплює захист інформації, що стосується військового потенціалу та інших аспектів національної безпеки. Недостатній захист життєво важливих інформаційних ресурсів та інформаційних і телекомунікаційних систем може створити загрозу міжнародній безпеці. Позиція ЄС з приводу інформаційної безпеки відзначається раціоналізмом, адже предметом безпеки називаються конкретні поняття різних видів інформації. Крім того, простежується досить чітке розмежування особливостей *інформаційної безпеки людини і суспільства* (особиста інформація, інформаційне забезпечення життя суспільства) та *інформаційної безпеки держави* (інформаційне забезпечення національної безпеки).

ІНФОРМАЦІЙНА БОРОТЬБА — комплекс заходів, які вживаються для досягнення інформаційної переваги над супротивником шляхом впливу на інформацію, якою він володіє, процеси, що залежать від інформації, інформаційні системи, комп'ютерні мережі з одночасним захистом від аналогічних впливів із боку противника *(визначення С.Жука)*. Вирізняються наступальна й оборонна складові інформаційної боротьби. На сучасному етапі постає нове завдання щодо впливу на супротивника ще в загрозливий період з тим, щоб забезпечити вигідний для держави напрямок процесів управління і прийняття рішень протилежною стороною.

ІНФОРМАЦІЙНА БОРОТЬБА (ЗАВДАННЯ) - отримання розвідувальної інформації шляхом перехоплення та розшифровування інформаційних потоків, що передаються через канали зв'язку, а також через побічні випромінювання, а також за рахунок спеціального втілення технічних засобів перехоплення інформації; отримання потрібної інформації шляхом перехоплення і обробки відкритої інформації, що передається через незахищені канали зв'язку, циркулює в інформаційних системах, а також: опублікованої у відкритих джерелах та ЗМІ; електромагнітний вплив на елементи інформаційних і телекомунікаційних систем; психологічний вплив, спрямований проти персоналу та осіб, що приймають рішення; формування і масоване розповсюдження через інформаційні

канали противника та глобальні мережі дезінформації та тенденційної інформації; вогневе придушення (у воєнний час) елементів інфраструктури державного і воєнного управління; здійснення несанкціонованого доступу до інформаційних ресурсів з подальшим їх викривленням, знищенням або викраденням, або порушенням нормального функціонування таких систем; захист від аналогічних впливів збоку противника.

ІНФОРМАЦІЙНА ВІЙНА - 1) дії, що вчинюються для досягнення інформаційної переваги у підтримці національної воєнної стратегії через вплив на інформацію та інформаційні системи противника при одночасному забезпеченні безпеки власної інформації та інформаційних систем; 2) нефізичну атаку на інформацію, інформаційні процеси та інформаційну інфраструктуру; 3) є найвищим ступенем інформаційного протиборства та спрямована на розв'язання суспільно-політичних, ідеологічних, а також національних, територіальних та інших конфліктів між державами, народами, націями, класами й соціальними групами шляхом широкомасштабної реалізації засобів і методів інформаційного насильства (інформаційної зброї) *(визначення С.Жука)*. Вперше термін «інформаційна війна» було введено в 1985 р. у Китаї. За основу теоретичних підходів китайських спеціалістів в області інформаційного протиборства були взяті погляди давньокитайського воєнного діяча Сунь-цзи. Він першим узагальнив досвід інформаційного впливу на супротивника. У трактаті «Мистецтво війни» Сунь-цзи писав: «У будь-якій війні, як правило, найкраща політика зводиться до захоплення держави в цілому... Одержати сотні перемог у бою - це не межа мистецтва. Підкорити супротивника без бою - ось це венець мистецтва». При цьому *інформаційна війна* включає наступні дії: *здійснення впливу на інфраструктуру систем життєзабезпечення* - телекомунікації, транспортні мережі, електростанції тощо; *промисловий шпіонаж* - порушення прав інтелектуальної власності, розкрадання патентованої інформації, викривлення або знищення важливих даних, проведення конкурентної розвідки; *хакінг* - злам і використання особистих даних, ідентифікаційних номерів, інформації з обмеженим доступом тощо. Цілі інформаційної війни є дещо іншими, аніж війни у звичному розумінні. Якщо за умов ведення *звичайної війни* головною метою є фізичне знищення противника і ліквідація його збройних сил, то за умови ведення *інформаційної війни* відбувається широкомасштабне порушення роботи фінансових, транспортних і комунікаційних мереж і систем, руйнування економічної інфраструктури і підкорення населення країни, що зазнала атаки, зміни світоглядних настанов, зародження сумніву у необхідності та доцільності існування в рамках самостійної, суверенної держави. Однією

з головних цілей інформаційної війни є пригнічення в людини морального творчого початку.

ІНФОРМАЦІЙНА ЕКСПАНСІЯ — діяльність по досягненню національних інтересів методом безконфліктного проникнення в інформаційну сферу з метою поступової, плавної, непомітної для суспільства зміни системи соціальних відносин за зразком системи джерела експансії; витіснення положень національної ідеології і національної системи цінностей і заміщення їх власними цінностями й ідеологічними установками; збільшення ступеня свого впливу і присутності, встановлення контролю над стратегічними інформаційними ресурсами, інформаційно-телекомунікаційною структурою і національними ЗМІ; нарощування присутності власних ЗМІ в інформаційній сфері об'єкта проникнення тощо.

ІНФОРМАЦІЙНА ЗБРОЯ - це пристрої та засоби, які призначені для нанесення протидіючій стороні максимальної шкоди в ході інформаційної боротьби (шляхом небезпечних інформаційних впливів). До «інформаційної зброї» належить, по-перше, засоби інформаційно-технічного характеру, які знищують, перекручують або викрадають інформацію, незважаючи на систему захисту, обмеження доступу до цієї інформації законних користувачів. По-друге, це безперечно, інформаційно-психологічні засоби, які дезорганізують інформаційні системи, шляхом дезінформації, формування помилкових логічних інформаційних концепцій, інтерпретацій та ін., впливаючи, таким чином, на суспільну думку, на життя суспільства, держави або групи держав в цілому. Об'єктами впливу можуть бути: *інформаційно-технічні* системи, які включають людину, *інформаційно-аналітичні* системи, які включають людину, *інформаційні ресурси,* системи формування суспільної свідомості та думки, яка базується на засобах масової інформації та пропаганди, а також психіки людини.

ІНФОРМАЦІЙНА ІНФРАСТРУКТУРА — сукупність компонентів, що забезпечують загальні умови функціонування та розвитку інформаційної сфери.

ІНФОРМАЦІЙНА ОПЕРАЦІЯ — система дій, що складається з наступних компонентів: 1. Operations Security (OPSEC) - захист інформації про план операції, про елементи, які суттєво впливають на досягнення успіху, про союзні сили задля уповільнення процесу прийняття рішення супротивником. (JP 3-54 «Joint Doctrine for Operations Security»). 2. Military deception - введення в оману. Використання усіх можливих засобів для введення в оману супротивника стосовно перебігу операції, ключових точок місцевості, напрямків основних зусиль. Уповільнює процес прийняття рішення супротивником через його системи збирання і аналізу ін-

формації. (JP 3-58 «Joint Doctrine tor Military Deception»). 3. Electronic Warfare (EW) - РЕБ. Використання спрямованої електромагнітної енергії для впливу на супротивника, та захист власних радіосистем. (JP 3-51 «Electronic Warfare in Join Military Operations»). 5. Physical attack / destruction - атака та фізичне знищення. Використання зброї проти визначених цілей для досягнення більшої ефективності інформаційної операції. 6. Computer network attack (CNA) - атака на комп'ютерні мережі. 7. Psychological Operations (PSYOP) - психологічні операції. Забезпечують умови для відновлення порядку, підтримку дружньо налаштованого населення. Вплив на супротивника та нейтралізація психологічного впливу з його боку. Психологічні операції повинні підтримувати заходи по введенню противника в оману. (JP 3-53 «Doctrine for Joint Psychological Operations»). 8. Public Affairs(PA) - суспільні відносини. Інформування власної та іноземної аудиторії про свої цілі, дружні війська, хід операції. PA не використовують для введення в оману чи розповсюдження дезин-формації. (JP 3-61 «Doctrine for Public Affairs in Joint Operations»). 9. Civil Affairs (CA) - цивільні відносини. Встановлення військовим командуванням дружніх стосунків з місцевими органами управління, населенням, місцевим лідерами районі своїх інтересів. CA & PSYOP можуть бути поєднані. (JP 3-57 «Doctrine for Joint Civil Affairs»). У мирний час, в умовах обмежень у використанні сил, способів і засобів кількість складових інформаційної операції зменшується до чотирьох. Computer network attack (CNA). Psychological Operations (PSYOP). Public Affairs(PA). Civil Affairs (CA). Це ті види інформаційного впливу, які несуть постійну загрозу інформаційній безпеці України. З них найбільш небезпечні це атаки на комп'ютерні мережі та психологічні операції *(визначення американських експертів з інформаційної боротьби).*

ІНФОРМАЦІЙНА ПЕРЕВАГА - перевага над супротивником в інформаційній сфері.

ІНФОРМАЦІЙНА ПОЛІТИКА ДЕРЖАВИ — діяльність держави в інформаційній сфері, спрямована на задоволення інформаційних потреб людини та громадянина через формування відкритого інформаційного суспільства на основі розвитку єдиного інформаційного простору цілісної держави та його інтеграції у світовий інформаційний простір з урахуванням національних особливостей і інтересів при забезпеченні інформаційної безпеки на внутрішньодержавному та міжнародному рівнях *(визначення Арістової І.В.).*

ІНФОРМАЦІЙНЕ ПРОТИБОРСТВО (злвдАння) - створення в країні противника атмосфери бездуховності, негативного ставлення до культурної спадщини; маніпулювання суспільною свідомістю і політичною орієнтацією

груп населення держави з метою створення політичної напруги і хаосу; дестабілізація політичних стосунків між партіями, об'єднаннями та рухами з метою провокації конфліктів, розпалення недовіри, підозрілості, загострення політичної боротьби, провокування репресій проти опозиції і навіть громадянської війни тощо; зниження рівня інформаційного забезпечення органів влади й управління, ініціація помилкових управлінських рішень; дезінформування населення про роботу державних органів, підрив їх авторитета, дискредитація органів управління; провокування соціальних, політичних, національних і релігійних зіткнень; ініціювання страйків, масових заворушень та інших акцій економічного протесту; ускладнення прийняття органами управління важливих рішень; підрив міжнародного авторитету та іміджу держави, її співробітництва з іншими країнами.

ІНФОРМАЦІЙНЕ ПРОТИБОРСТВО (поняття) - 1) суперництво соціальних систем (країн, блоків країн) в інформаційній сфері з приводу впливу на ті або інші сфери соціальних відносин і встановлення контролю над джерелами стратегічних ресурсів, у результаті якого одна група учасників суперництва отримує переваги, необхідні їм для подальшого розвитку, а інша їх втрачає; 2) форма боротьби сторін в інформаційному просторі з використанням політичних, економічних, дипломатичних, військових та інших методів, способів та засобів для впливу на інформаційне поле супротивника та захисту власного інформаційного поля в інтересах досягнення поставлених цілей.

ІНФОРМАЦІЙНЕ ПРОТИБОРСТВО (ФОРМИ) - політичні, дипломатичні й економічні акції; інформаційні та психологічні операції; підривні і демо-ралізуючі пропагандистські дії; сприяння опозиційним і дисидентським рухам; надання усебічного впливу на політичне і культурне життя з метою розвалу національно-державних підвалин суспільства; проникнення в систему державного керування.

ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО - 1) громадянське суспільство з розвинутим інформаційним виробництвом і високим рівнем інформаційно-правової культури, в якому ефективність діяльності людей забезпечується розмаїттям послуг на основі інтелектуальних інформаційних технологій та технологій зв'язку *(визначення Арістової І.В.);* 2) суспільство нового типу, що формується внаслідок глобальної соціальної революції та породжується вибуховим розвитком і конвергенцією інформаційних та комунікаційних технологій; суспільство знання, тобто суспільство, в якому головною умовою добробуту кожної людини і кожної держави стає знання, здобуте завдяки безперешкодному доступу до інформації та вмінню працювати з нею; глобальне суспільство, в якому обмін ін-

формацією не буде мати ані часових, ані просторових, ані політичних меж; яке, з одного боку, сприятиме взаємопроникненню культур, а з іншого - відкриватиме кожному співтовариству нові можливості для самоідентифікації *[визначення Європейської комісії);* 3) суспільство, в якому основним предметом праці переважної більшості людей стають інформація й знання, тобто інформаційні ресурси, знаряддям праці -комп'ютерна техніка, засобами - інформаційні технології *(визначення Гурковського В.І.);* 4) суспільство, в якому діяльність людей здійснюється на основі використання послуг, що надаються за допомогою інформаційних технологій та технологій зв'язку.

ІНФОРМАЦІЙНИЙ КОЛОНІАЛІЗМ - експлуатація інформаційного простору держави іншими країнами за рахунок суцільного використання імпортних інформаційних технологій і високотехнологічної техніки і устаткування.

ІНФОРМАЦІЙНІ ПРАВА ТА своводи — нормативно закріплені права та свободи громадян в інформаційній сфері.

ІНФОРМАЦІЙНИЙ ПРОДУКТ — документована інформація, підготовлена та призначена для задоволення потреб користувачів.

ІНФОРМАЦІЙНІ РЕСУРСИ — 1) сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо); 2) організована сукупність інформаційних продуктів певного призначення, що необхідні для забезпечення інформаційних потреб громадян, суспільства, держави у певній сфері життя чи діяльності.

ІНФОРМАЦІЯ - 1) відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб; 2) документовані або публічно оголошені відомостей про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі; 3) аналітично оброблені дані.

ІНФРАСТРУКТУРА - 1) сукупність галузей народного господарства, що забезпечують загальні умови функціонування економіки і життєдіяльності людей; 2) сукупність споруджень, будинків, систем і служб, необхідних для функціонування галузей матеріального виробництва і забезпечення умов життєдіяльності суспільства.

ІНФРАСТРУКТУРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ - сукупність підсистем забезпечення інформаційної безпеки, що формують загальні умови функціонування системи національної безпеки.

КІБЕРЗЛОЧИННІСТЬ - злочинність у кібернетичному (віртуальному) просторі - просторі комп'ютерно-телекомунікаційних мереж.

КОДИФІКАЦІЯ ІНФОРМАЦІЙНОГО ПРАВА - приведення чисельних норм в узгоджену систему на основі загальновизнаних принципів права.

Комерційна таємниця — відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами тощо, що не є державними таємницями, розголошення (передача, витік) яких може завдати шкоди його інтересам. Склад і обсяг відомостей, що становлять комерційну таємницю, порядок їх захисту визначаються керівником підприємства.

Конфіденційна інформація - вид інформації з обмеженим доступом, інформація, що перебуває у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб, які можуть поширюватися за їх бажанням відповідно до передбачених ними умов.

НлцюБКзиккознлвство (поняття) (від лат. *natio* - плем'я, народ; від укр. *безпека, ...juaecmeo* - наука, вчення, течія) - 1) суспільна міждисциплінарна наука, яка досліджує загальні та специфічні об'єктивні закономірності організації та функціонування системи національної безпеки, виробляє на підставі її пізнання загальні теоретичні положення, що спрямовані на підвищення ефективності функціонування даної системи, належить до наук безпекознавчого циклу; 2) теоретична система ідей, поглядів та уявлень про шляхи реалізації національної безпеки творення з метою забезпечення гарантій національних інтересів, що відображають об'єктивний процес існування тріадичного організму: особа, суспільс тво, держава; 3) концепція розвитку національної безпеки на дуалістичній основі, що визначається у форматі системи національної безпеки; 4) проблема реалізації національної ідеї безпекотворення; 5) комплексна наука, що вивчає національну безпеку; 6) галузь безпекознавства, об'єктом якої є національна безпека; 7) система знань, що мають своїм предметом національну безпеку як цілісний екзистенціальний феномен; 8) сукупність чисельних концептуальних узагальнень, котрі представлені полемізуючими між собою теоретичними школами і які складають предметне поле відносно автономної дисципліни; 9) наукова система знань про теорію і практику специфічного виду діяльності суб'єктів забезпечення національної безпеки України, яка узагальнює і пояснює її, виявляє закономірності розвитку даної діяльності з метою її удосконалення, виходячи із об'єктивної потреби у забезпеченні безпеки особи, сус -пільства і держави як цілісного організму; 10) логічна взаємопов'язана і взаємообумовлена система категорій, понять та принципів, які інтерпретують сутність (зміст та генезис) національної безпеки в Україні; 11) система знань про найбільш загальні поняття, принципи та інститути, характерні для всіх наукових напрямів і теорій національної безпеки, воно вивчає національну безпеку на макрорівні, як систему в цілому, безвідносно до галузевих особливостей національної безпеки.

НАЦІОНАЛЬНА БЕЗПЕКА - форма соціальної діяльності, свідомий цілеспрямований вплив суб'єкта управління на загрози та небезпеки, за якого державними та недержавними інституціями створюються необхідні і достатні умови для прогресивного розвитку українських національних інтересів, джерел добробуту народу України, а також забезпечується ефективне функціонування системи національної безпеки України.

НАЦІОНАЛЬНА ІДЕЯ - 1) охоплююча всі прошарки нації у всьому її розмаїтті Ідея, інтегруючий чинник націо- і державотворчого процесу; 2) сукупність найважливіших, ключових, фундаментальних уявлень про цілі, завдання та перспективи розвитку особи (індивіду), суспільства та держави; 3) ідеологія розвитку нації - держави, система поглядів, ідей та цінностей, сформульована і загальноприйнята мрія; 4) мета, мотивація діяльності, ключовий елемент суспільної свідомості, менталітет, формула поведінки.

НАЦІОНАЛЬНИЙ ІДЕАЛ - і) ідейна основа, найбільш загальні уявлення нації стосовно об'єктивних тенденцій реальної дійсності про її соціально-економічний і духовний розвиток, гармонійна єдність суб'єкта й об'єкта, окремого представника, нації в цілому та природи, які знаходять вираз у вільному й універсальному розвиткові нації і становлять собою кінцеву мету її прагнень і діяльності; 2) органічне поєднання волі представника нації, вираженої в національній ідеї.

НАЦІОНАЛЬНІ ІНТЕРЕСИ - 1) результат усвідомлення цінності потреб, свідомий вибір національних цінностей, які обумовлені національним ідеалом, метою та ідеєю і забезпечують умови та засоби їх задоволення та реалізації; 2) обумовлена національним ідеалом, національною метою та національною ідеєю система загальнозначимих, усвідомлених та визнаних потреб і національних цінностей, яка забезпечує умови та засоби їх задоволення і реалізації; 3) сукупність політичних, економічних, соціальних та інших потреб нації, від реалізації яких залежить здатність держави забезпечити захист конституційний прав людини і громадянина, цінностей українського суспільства, основоположних державних інститутів; 4) усвідомлені особою і суспільством, гарантовані державою цільові настанови щодо необхідності існування та розвитку людини, нації і держави як цілокупного організму; 5) свідомісний вибір людиною національних цінностей; 6) сукупність усвідомлених, офіційно відображених в конституції, законах, концепціях, стратегіях та інших нормативних актах об'єктивних потреб громадян, суспільства та держави, які є похідними від національних цінностей, особливостей та умов соціально-економічного і політичного устрою держави, рівня її економічного розвитку та місця і ролі у міжнародному розподілі праці,

специфіки історичного розвитку та географічного положення; 7) життєво важливі матеріальні, інтелектуальні й духовні цінності українського народу як носія суверенітету і єдиного джерела влади в державі, визначальні потреби суспільства і держави, реалізація яких гарантує державний суверенітет країні та її прогресивний розвиток *(законодавче визначення)*.

НАЦІОНАЛЬНІ ІНТЕРЕСИ В ІНФОРМАЦІЙНІЙ СФЕРІ - життєво важливі матеріальні, інтелектуальні й духовні цінності народу як носія суверенітету і єдиного джерела влади в державі, визначальні інформаційні потреби суспільства і держави, реалізація яких гарантує: інформаційний суверенітет країни; вдосконалення державного регулювання розвитку інформаційної сфери, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації до боротьби з організованою злочинністю *та* корупцією, зловживанням службовим становищем, іншими явищами, які загроясують національній безпеці України; неухильне дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері та переслідування журналістів за політичні позиції; створення необхідних і достатніх умов для нормального функціонування та розвитку національного інформаційного простору; унеможливлення монополізації інформаційної сфери України.

НОРМИ ІНФОРМАЦІЙНОГО ПРАВА - це юридично обов'язкові до виконання правила поведінки держав та інших суб'єктів міжнародного права, що встановлюються самими суб'єктами міжнародного права і виконуються ними добровільно чи за необхідності з допомогою особливого виду примусу.

ОДЕРЖАННЯ ІНФОРМАЦІЇ - набуття, придбання, накопичення інформації громадянами, юридичними особами або державою відповідно до чинного законодавства України.

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ - діяльність державних, недержавних, міжнародних та наддержавних інституцій, спрямована на організацію оптимального управління загрозами та небезпеками в інформаційній сфері з метою своєчасного виявлення загроз та небезпек національним інтересам в інформаційній сфері, визначення стратегічних завдань із забезпеченню національної безпеки в інформаційній сфері, удосконалення системи забезпечення інформаційної безпеки, її

сил та засобів, створення мобілізаційних ресурсів і визначення порядку їх розгортання.

ПОШИРЕННЯ ІНФОРМАЦІЇ – розповсюдження, оприлюднення, реалізація інформації у встановленому законом порядку.

ПРАВА І СВОБОДИ В ІНФОРМАЦІЙНІЙ СФЕРІ ЄВРОСОЮЗУ - права, які закріплюються в Хартії основних прав Європейського Союзу, базуються на конституційних традиціях та загальних міжнародних зобов'язаннях держан-членів, а також Договору про Європейський Союз, Договору про Європейські співтовариства, Європейській конвенції про захист прав людини та основних свобод, Соціальних хартіях, прийнятих Європейським співтовариством й Радою Європи, та судової практики суду Європейських співтовариств та Європейського суду з прав людини.

ПРАНО ВЛАСНОСТІ НА ІНФОРМАЦІЮ - врегульовані законом суспільні відносини щодо володіння, користування і розпорядження інформацією.

ПРАВО НА ІНФОРМАЦІЮ - 1) можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій; 2) самостійно конституційне право, яке дозволяє людині вільно збирати, зберігати, використовувати і поширювати інформацію будь-яким способом, що гарантується *(ч. 2 ст. 34 Конституції України)*.

РЕЖИМ ДОСТУПУ ДО ІНФОРМАЦІЇ - передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації.

Сили ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ - органи спеціальної компетенції, які з метою забезпечення інформаційної безпеки наділені державою правом на застосування прийомів те методів ведення інформаційної боротьби, Утворюються і розвиваються відповідно до рішень Президента України та Кабінету Міністрів України для виконання короткотермінових і довготривалих програм забезпечення інформаційної безпеки, реалізації внутрішньої та зовнішньої політики держави. Вони можуть включати в себе спеціальні підрозділи інформаційної боротьби у складі: Збройних сил України, Міністерства внутрішніх справ України, Внутрішніх військ МВС України, Служби безпеки України, Державної прикордонної служби України, Державної митної служби України, Управління державної охорони України, Міністерства закордонних справ України, інших військ, воєнних формувань та відомств, структурних підрозділів органів виконавчої влади, недержавні інституції, на які покладені функції із забезпечення інформаційної безпеки, а також законодавче передбачено порядок ведення інформаційної боротьби.

Сиїткмл заьі.зпкчкіша інформаційної вк:шкки — державні, недержаній та міжнародні органи та організації, посадові особи та окремі громади пи, об'єднані цілями й завданнями щодо створення сприятливих умов для реалізації інформаційних потреб, інтересів і цінностей, які взаі модіють один з одним і здійснюють відповідну діяльність згідно з пор мами міжнародного права і відповідними домовленостями.

Система інформаційної безпеки - множина інформаційних потреб, інтересів і цінностей осіб, суспільств і держав, загроз та небезпек, внутрішніх та зовнішніх, об'єктивних та суб'єктивних, природних, техногенних та антропогенних чинників, що впливають на рівень інформаційної безпеки, умови їх гоненії, еволюції та балансу, державні, міжнародні та недержавні інституції, об'єднані цілями і завданнями щодо створення сприятливих умов для реалізації інформаційних потреб, інтересів і цінностей, які взаємодіють один з одним і здійснюють відповідну діяльність згідно з нормами міжнародного права і відповідними домовленостями.

Структура права па інформацію - внутрішня будова права на інформацію, що визначається такими складовими як: одержання інформації; зберігання інформації; використання інформації; поширення інформації.

Тємнл інформація - вид інформації з обмеженим доступом, інформація, іцо містить відомості, які становлять державну та іншу, передбачену Законом таємницю, розголошення якої завдає (чи може завдати) шкоду особі, державі, суспільству.

Навчальне видання

В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховськии

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ЄВРОШТЕГРАЦІЇ

Навчальний посібник *Серія:*

Національна і міжнародна безпека

Керівник видавничих проектів *Кривенко О. А.*
Відповідальний за випуск *Пашутинський Є. К.*
Художнє оформлення *Бажина В. С.*

Підписано до друку 09.06.2006 р.
Гарнітура SchoolBookAC. Формат 60х84 / .
Папір офсетний. Друк офсетний.
Обл.-видав, арк. 19,97. Умов. друк. арк. 16,27.
Тираж 1000 пр.

Видавництво КНТ м. Київ, пр. Героїв Сталінграда, 8, корп. 8, кв. 1
Тел./факс (044) 581-21-38
e-mail: knt2003@ukr.net, www.knt2005.narod.ru
Свідоцтво: серія ДК № 581 від 03.08.2001р.

Друкарня ПП «МРІЯ-ДРУК»
м. Харків, вул. Балакірева, 20-270

Зам. № fSloe