

і і. -™

O.B.COCHIN

•I

» №

11 •I •

**ПРОБЛЕМИ
ДЕРЖАВНОГО
УПРАВЛІННЯ
НАЦІОНАЛЬНИХ
ІНФОРМАЦІЙНИХ РЕСУРСІВ
ПОТЕНЦІАЛУ
УКРАЇНИ**

\.-v

•••v

i 1_{Hv} " *.

i ,

Г «., •

ч • « I

•fl I I i , '

\ ;•• Ши*

'1 '

* } ,

•v • \ v/-..^

**ІНСТИТУТ ДЕРЖАВИ І ПРАВА ім. В.М. Корецького
НАЦІОНАЛЬНОЇ АКАДЕМІЇ НАУК УКРАЇНИ**

О.В. Соснін

**ПРОБЛЕМИ
ДЕРЖАВНОГО
УПРАВЛІННЯ
СИСТЕМОЮ НАЦІОНАЛЬНИХ
ІНФОРМАЦІЙНИХ РЕСУРСІВ
З НАУКОВОГО ПОТЕНЦІАЛУ
УКРАЇНИ**

І І

УДК 347.778
ББКХ621.152

С 66

Ц
Є ^

Рекомендовано до друку
Вченою радою Інституту держави і права
ім. В.М. Корейського НАН України

Рецензенти:

В.П.Горбатенко, доктор політичних наук, професор;
Є.А.Макаренко, доктор політичних наук, професор;
Г.М.Перепелиця, доктор політичних наук, професор;
С.О.Шергін, доктор політичних наук, професор

Соснін О. В.

*" °° Проблеми державного управління системою національ-
них інформаційних ресурсів з наукового потенціалу
України: Монографія. — К: Інститут держави і права
ім. В.М.Корецького НАН України, 2003. — 572 с
ISBN 966-02-3096-6

У монографії висвітлюються проблеми й основні напрями
світового розвитку інформаційної сфери і ринку послуг, пов'я-
зані з обігом інформації в глобальному просторі. Саме обіг інфор-
мації формує інформаційне суспільство, інтенсивно впровад-
жуючи досягнення науки і техніки у виробництво і побут людей.
Аналізуються організаційно-правові засади і механізми відтво-
рення та захисту науково-технічного потенціалу України у гло-
бальному інформаційному середовищі. Пропонуються шляхи
вдосконалення управління системою національних інформацій-
них ресурсів, які розглядаються як головний ресурс розвитку
інноваційної політики Української держави.

Розрахована на науковців, працівників інформаційної сфе-
ри, студентів та широке коло читачів.

Б Б К Х 621.152

Національна бібліотека України
імені Ізидора Верналового

Акт № 217&~/

ISBN 966-112-3096-6

2.003

© Соснін О.В., 2003

Від автора

Вражаючий прогрес у галузі інформаційних технологій, до-
сягнутий упродовж останніх п'ятдесяти років завдяки стрімко-
му розвитку електронно-обчислювальної техніки, дещо дефор-
мував уявлення про мету і сутність інформаційної революції,
зробивши наголос на інформаційних технологіях. Справді, бур-
хливий розвиток електронної й електротехнічної промисловості,
наукові основи яких було закладено ще в ХІХ столітті для
потреб створення військових засобів зв'язку, сприяв прискоре-
ному розвитку інформатизації суспільства. Завдяки темпам її
розвитку комп'ютер дав змогу подвоювати людські знання щорічно, а в недалекій перспективі, за прогнозами, це відбувати-
меться щомісячно.

Шумерська цивілізація (3 тис. років до РХ) залишила на-
щадкам чимало пам'яток писемності — зібрання глиняних таб-
личок. Єгипетська — значну кількість папірусів. Стародавня
Греція подарувала нам саме слово «бібліотека», а дім Арісто-
теля став домом читача. Найвідомішою в античну епоху була
Александрійська бібліотека, фонди якої, за різними оцінками,
нараховували від 100 до 700 папірусних свитків¹.

Наша перша відома бібліотека Ярослава Мудрого, близько
1037 року, бібліотеки монастирів і особисті зібрання рукописів
князів, митрополитів дали підстави вважати Київську Русь ци-
вілізованою державою.

Найбільші бібліотеки світу подвоюють свої запаси кожні чо-
тиринадцять років, тобто зростають у 140 разів кожне століття,
ще на початку ХНІ століття бібліотека Сорбонни вважалася най-
більшою в Європі (вона містила 1338 книжок), а сьогодні щоден-

не видання великої газети, наприклад «Нью-Йорк Тайме», містить більше інформації, ніж середній європейець XVII століття засвоював за своє життя.

Як свідчать розрахунки експертів, на початку XX століття «обсяг знань» подвоювався кожні 50 років. Упродовж останніх 30 років було створено незникаючого людського ресурсу — знання — продукту сучасної цивілізації, її головної рушійної сили, більше нової інформації, ніж за попередні 5 тисяч років.

Звернемо увагу на такі факти. Відповідно до новітніх розрахунків, які наводяться в Британській енциклопедії, кількість книжок, що видавалися в Європі в XVI столітті, подвоювалася кожні сім років. Припустимо, якщо в 1500 році було видано три книжки, у 1507 — 6, у 1514 — 12, то в 1598 — уже 49 152.

Це геометрична прогресія зі знаменником 2. Насправді до 1500 року, незважаючи на те, що друкарський верстат працював лише піввіку, було видано не 3 книжки, а 9 мільйонів книжок (стаття «Книговидання» у тій же Британській енциклопедії). Цікаво, що з такою ж швидкістю — подвоюючись за семирічний проміжок — зростає незалежно підрахований глобальний обсяг науково-технічної літератури в XX столітті. За іншими підрахунками, обсяг знання, виробленого в друкарській формі, подвоюється кожні вісім років². А ось середня тривалість життя за 400 років збільшилася не геометрично, а лише арифметично, не більш як удвоє*.

Нині ще дуже важко гадати, якими будуть наслідки цього — за законами об'єктивної діалектики вони нестимуть у собі і добро, і зло, оскільки пересічна людина — індивід усе більше відчувається неадекватною у відносинах з навколишнім інформаційним середовищем: зір і слух зазнають значного навантаження, якого не витримують мозок і **серце, оскільки** між людиною, чії можливості біологічно обмежені, та людством, що необмежене у своїй техно-інформаційній експансії, виникає своєрідний дисбаланс. Бурхливі потоки дрібних інформаційних часточок без-

* Середня тривалість людського життя на початку нашої ери становила 20 — 25 років, наприкінці XVIII століття — 35 — 40 (у Західній Європі та Північній Америці). Див. статтю «Біологічний зріст і розвиток» у Британській енциклопедії.

перестану бомбардують нашу свідомість, спричиняючи оніміння й омертвіння розумових та й сприйнятливих спроможностей. Можна передбачати настання часу, коли тільки виняткові індивіди будуть спроможні відповідати рівню інформаційного розвитку цивілізації, тобто бути воістину цивілізованими і воістину людьми. Потім відстануть і вони — і цивілізація помчить уперед, уже не просто ніким не керована, але в цілому і ніким не сприймана, як могутній і нестримний вихор. Між людиною і людством стає дедалі менше спільного, так що втрачає первісний зміст навіть сам кореневий зв'язок цих двох слів.

Мінімізація негативних і посилення позитивних наслідків потребують ряду наукових, гуманітарних, соціальних і інженерно-технологічних проблем, здійснення відповідних досліджень у суспільстві.

Україні потрібна свідомо, на рівні національного пріоритету номер один, виважена державна політика розвитку науки і технології. Тільки визнання нами суперпріоритетом високих інноваційних, у широкому розумінні, сучасних наукомістких технологій, в основі яких лежать фундаментальні науки, може вивести Україну на лінію сучасних глобальних трансформацій, де форсований прорив у майбутнє роблять передові країни. Перетворення України на суспільство сучасних високих інноваційних технологій, що є не тільки основою національної безпеки, дало б можливість розв'язати відразу кілька фундаментальних проблем:

- підвищити рівень національної освіченості й кваліфікації як головного джерела добробуту, стабільності та культури;
- ефективніше розв'язувати проблеми охорони здоров'я, екології та демографії;
- зберегти територіальну цілісність країни, єдиний економічний і соціокультурний простір.

. Такий прорив водночас означав би активне включення України до системи транскультурних і трансцивілізаційних зв'язків, характерних для сучасного етапу процесу глобалізації. Досвід минулого століття, «економічне чудо» в Японії й Німеччині, вражаючи успіхи Південної Кореї і Китаю підтверджують, що випереджальний розвиток науки і технологій та впровадження їхніх результатів у політичну, соціокультурну й економічну практику дасть змогу нам, незважаючи на катаклі-

зми минулих років, ввести в господарський обіг країни значну частину свого дуже постраждалого, але усе ще значного науково-технічного потенціалу. Реалізація цього сценарію за умови координації зусиль держави і бізнесу — аж ніяк не утопія, а реалістична можливість.

Сьогодні саме на державному рівні потрібна постійна робота по удосконаленню системних організаційно-правових засад функціонування інформаційних ресурсів, насамперед науково-технічної інформації, щоб створити адекватні моделі поєднання економічних, виробничих і наукових інтересів країни, оскільки, володіючи значним інтелектуальним, а відтак і інформаційним ресурсом, ми завжди маємо перспективу прогресу і можливість зайняти гідне місце у світовому співтоваристві, забезпечити достатній науково-технологічний потенціал, вжити заходів із захисту національних інтересів у будь-якій сфері життєдіяльності.

«Інформація» дедалі більше усвідомлюється як стратегічний ресурс і є сутнісною складовою цього процесу. Проблемою є саме розуміння, усвідомлення феномену під назвою «інформаційний ресурс». Це поняття, як і поняття «інформація», сприймається нами переважно на інтуїтивному рівні, вони ототожнюються навіть у офіційних документах, як сукупність відомостей, зафіксованих на матеріальних носіях. Водночас інформаційні ресурси держави — це сукупність бібліотечних, у загальному розумінні, фондів доробку інтелектуальної праці людства.

Можна стверджувати, що саме розвиток електронної техніки засобів зв'язку зумовив інформатизацію нашого суспільства і водночас створив складне інформаційне середовище з численними джерелами одержання інформації і засобами її уявлення та передавання. Управління подібним інформаційним середовищем у національних інтересах чекає свого розв'язання, оскільки являє собою проблему виключної складності.

Світ давно зрозумів, що інформація перетворилася на реальну силу, стала основним інструментом управління критично важливими структурами суспільства і держави. Багато політичних діячів на конкретних прикладах транскордонних інформаційних операцій, у тому числі безпосередньо терористичного і військового характеру, довели, що нова загроза, або так звана неіснуюча війна, набула реальних обрисів.

Усвідомлюючи всю серйозність потенційної загрози впливу на свої інформаційні ресурси, провідні країни на національному рівні почали реалізацію довгострокових державних програм, спрямованих на забезпечення інформаційної безпеки передусім критично важливих інфраструктур.

Вочевидь, настав час, коли міжнародному співтовариству необхідно реально досягти чіткого розуміння проблеми глобальної взаємозалежності національних інформаційних ресурсів у всій її повноті й комплексності, визнати, що успіх національних зусиль по охороні свого інформаційного ресурсу залежить від рівня захищеності і «неагресивності» інформаційних просторів інших, у тому числі несусідніх, держав, із якими їхні інформаційні ресурси об'єктивно пов'язані.

Всесвітня федерація вчених, свого роду «мозок людства», у серпні 2000 року першою в списку загроз людству в XXI столітті поставила загрозу міжнародної інформаційної безпеки (МІБ), відтіснивши на другий план екологію, енергетику й інші постійно обговорювані теми, а події вересня 2001 року в США закріпили це у свідомості людства. Вмить безпека інформаційного простору стала загальнолюдською проблемою, ожививши в пам'яті глобальні конфлікти, супроводжувані активними діями СІЛА і НАТО, скандали навколо «Ешелону», тисячі кібернетичних атак на інформаційні і керуючі системи економічних і політичних структур різних країн, Інтернет, який сприймається як інструмент формування нової свідомості інформаційного суспільства. Світ одержав можливість відповідально виражати свої уявлення про роль інформації у світі, про мир і війну в інформаційній сфері.

Нам ще належить усвідомити, що змістовний інформаційний ресурс, а це зареєстровані відповідним чином відомості про наукові знання і стан соціально-економічного розвитку, які створені або виявлені, мають визначені закономірності деградації й оновлення, і, що інформаційний продукт, який є предметом споживання суспільства, має бути відповідним чином оцінено і захищено.

Проблеми формування, поширення і використання не взагалі інформації, а змістовного інформаційного ресурсу стали для України сьогодні особливо актуальними тому, що ми маємо залучити їх для підвищення своєї конкурентоспроможності.

На початку XXI століття людство переживає інформаційний вибух, основною жертвою якого стали останні два — три покоління, коли наступ великої інформаційно-технологічної революції став наймогутнішим. Не призменшуючи ролі технологічної складової науково-технічної революції, підкреслимо роль її інформаційної складової: перш ніж вести мову про те, «як передавати», треба мати «що передавати». За такої постановки питання на перший план висувуються проблеми формування, поширення і використання не взагалі інформації, а змістовного інформаційного ресурсу, який є рушійною силою в усіх без винятку сферах суспільно корисної діяльності.

Автор ризикує, тому що будь-які інтерпретатори реалій сучасного розвитку суспільства й особливо тих питань, які прямо чи опосередковано пов'язані з інформаційним відтворенням наукових здобутків, спробують дещо іронічно ставитись до праці, яка пропонується. Своє завдання автор вбачає, по-перше, в тому, щоб висловити думки, більш-менш прийнятні для фахівців, але такі, що зазвичай не сприймаються непрофесіоналами — без цього навряд чи можна обґрунтувати предмет дослідження. По-друге, дати можливість відчувати справжню вагу питань інформаційної діяльності в умовах реформування економіки України, без претензій на первісність запропонувати деякі підходи до вирішення конкретних питань сьогодення.

Підтвердяться чи ні запропоновані думки та погляди, покаже час. Нині ж ці підходи мають відіграти свою роль у тому, що автор має намір не переконати читача у слушності конкретних відповідей на ряд гострих питань, викликаних новим підходом, а допомогти йому відчувати справжню їхню вагомість для особистості, суспільства, держави.

Автор висловлює щиру вдячність усім, хто своїми порадами і конкретною допомогою сприяв роботі над монографією та її опублікуванню, передусім Л. Є. Шиманському, Й. У. Мастяниці і В.К. Туровському. Особливо автор вдячний О.О. Кожемякіну та М.В. Яковлевій за допомогу у виданні.

З повагою до читача
Олександр Соснін

ВСТУП

Сьогодення України характеризується змінами в технічній, інформаційній і економічних сферах, зумовлених збігом історичних подій світового масштабу: не справдилися сподівання людства на процвітання після розпаду соціалістичного табору і біполярного світу; глобальне військове протистояння поступилося місцем зіткненню геополітичних інтересів великих держав у стратегічно важливих регіонах світу. Виявилось, що загроза атомної війни головним чином стримувала релігійні, расові та інші інстинкти людства, а підготовлений провідними країнами науково-технічний прорив, який здійснила інформаційно-комп'ютерна індустрія впровадженням глобальних інформаційних систем і використанням технологій програмування складних суспільних і економічних процесів, не принесла бажаної стабільності, перетворила світ на важкопрогнозовану для регулювання суспільних відносин структуру.

Включення України до світової економічної системи, наближення до неї кордонів Європейського Союзу і організаційна діяльність щодо формування євразійських структур активізує пошук форм взаємодії у стратегічних напрямках розвитку взаємовідносин з названими інтеграційними утвореннями, створює передумови для широкомасштабного співробітництва з ними. Вплив їх політичних інституцій зумовлює необхідність проведення послідовного процесу адаптації вітчизняної правової бази, економічних структур і всього господарського механізму до жорстких умов, що їх ставить світова ринкова економіка, формувати нові засади політичного і адміністративного устрою, оскільки Україна розташована на межі двох великих цивілізацій-

них просторів (євроатлантичного та євразійського), тому основне геополітичне питання, що постає перед країною, звучить так: чи спроможна вона реалізувати свої конкурентні переваги в глобальному географічному, інформаційному й економічному просторі?

Тільки з огляду на те, що Україна має розгалужену мережу вищих навчальних закладів, академічних і галузевих наукових центрів й інститутів, ми маємо шанс бути з-поміж держав, що живуть переважно за рахунок виробництва знань і створення сучасних наукоємних і високих технологій. Величезний науково-технологічний досвід, накопичений у державі, спроможний стати системоутворюючим чинником нашого поступу уперед. Науково-технічний потенціал України — це насамперед висококваліфіковані наукові й інженерно-технічні кадри, які мають володіти відповідною мотивацією до ефективної інтелектуальної творчої праці. Розвиток соціальної системи відбувається, поки існує «критична маса» вчених, здатних відображати науковий рух людства, підтримувати науковий і винахідницький потенціал для створення базових технологій шостого технологічного укладу. Вона катастрофічно зменшується, і тому для її збереження терміново необхідно мобілізувати наявні і потенційні можливості, щоб не залишитися на периферії під наглядом високотехнологічних транснаціональних корпорацій сировинним придатком і ринком збуту продукції світових виробників.

Сьогодні в Україні державна інноваційна діяльність зведена до ледь помітного мінімуму, високотехнологічні виробництва у промисловості поступово припиняють своє існування, наукові й інженерно-технічні кадри належним чином не задіяні, потенціал, що становить найважливішу частину національного багатства, швидко тоне і вже багато в чому втрачений. За десять років незалежності Україна не стала рівноправним суб'єктом науково-технічної співпраці і є лише постачальником кваліфікованої робочої сили, яка власне формує інтелектуальний потенціал розвинутих країн. Ситуація, в якій ми перебуваємо, досить суперечлива — з одного боку, існує потужний, багатівіковий, напрацьований попередніми поколіннями, науковий, освітній, промисловий потенціал нації, зберігаються історичні традиції культурних зв'язків і духовної спільності народів, з іншого — не затребуваний належним чином потенціал не відрод-

жується, руйнується експортною залежністю промислового виробництва, освіти, охорони здоров'я.

Починаючи з 2000 року, в Україні здійснено ряд реальних кроків у напрямі позитивних зрушень у державній науково-технічній політиці: проголошено про перехід на інноваційну модель розвитку економіки; затверджено Концепцію науково-технологічного та інноваційного розвитку України; прийнято зміни до Закону України «Про наукову і науково-технічну діяльність».

Реалізація заходів щодо вдосконалення функціонування науково-технологічної сфери України з метою створення конкурентоспроможної продукції при застосуванні сучасних технологій передбачає, що їх основними завданнями є:

- забезпечення безумовного виконання положень Закону України «Про наукову і науково-технічну діяльність», насамперед у частині бюджетного фінансування наукової і науково-технічної діяльності на рівні, не менше 1,7% ВВП ;
- розробка та впровадження програм структурної та технологічної модернізації науково-технічного потенціалу, приведення тематичного фронту НДДКР у відповідність до потреб виробничої сфери;
- створення на законодавчому рівні сприятливих умов для різних форм інтеграції науки і виробництва, зокрема, через механізми бюджетної, кредитно-фінансової, податкової, митної політики, сприяння розвитку інноваційних процесів;
- формування нормативно-правових механізмів введення об'єктів інтелектуальної власності до господарського обігу;
- функціонування інформаційно-аналітичної системи моніторингу науково-технічної діяльності в Україні.

У цьому контексті розвиток державності України безпосередньо пов'язаний з розвитком науки, сучасної інформаційної

У 1986 фінансовому році витрати Японії на НДДКР становили майже 9197 трлн. йен, що становить 2,75% ВВП. За витратами на НДДКР Японія відстає лише від США. Основну частку витрат на НДДКР в Японії несе приватна промисловість, частка державного фінансування постійно зменшується і становила у 1984 — 1985 фінансовому році 19,4%. *Терещенко В. И.* Проблема выбора: Политика научных приоритетов на Западе. — К.: Политиздат Украины, 1989. — С. 92.

інфраструктури, що забезпечують оперативний зв'язок щодо застосування новітніх знань та передових технологій для реалізації будь-якого виду людської діяльності.

На жаль, у всі періоди існування цивілізації люди існуючою політичною системою своїх країн завжди були орієнтовані на розв'язання проблем захисту своїх держав від агресії, політика держав вважалася вдалою, якщо досягнення науково-технічного прогресу впроваджувалися у військові проекти, що можна простежити на прикладі ведення бойових дій у різних регіонах світу.

Ми звикли, що протягом останніх десятиліть в Україні наука була тісно пов'язана з розв'язанням проблем національної оборони. Маючи прямі бюджетні асигнування, оборонна промисловість владно створювала промислову і наукову інфраструктуру країн регіонів, порушуючи баланс і зміщуючи соціальні інтереси.

Україна має великий науково-технічний досвід у сфері розробки і впровадження технологій оборонно-промислового комплексу, оскільки радянський період розвитку науки в Україні зумовлював створення, в умовах відносної ізоляції СРСР, могутнього наукового комплексу, здатного забезпечувати вирішення завдань оборони і безпеки, обслуговуючи потреби форсованого розгортання воєнної промисловості, а також інтенсивної індустріалізації країни. Були створені умови для проведення широкого фронту фундаментальних і прикладних досліджень, які охоплювали майже всі сфери знання.

Вочевидь, що прискорення науково-технологічного прогресу і впровадження в національну економіку більш високих технологій, ніж у країнах-конкурентах, є умовою збереження Україною статусу індустріальної держави в сучасному світі. Саме тому стільки дискусій виникає довкола проблеми використання досягнень науково-технічного потенціалу, його ролі для нашої країни. Але навіть прихильники науково-технічного прогресу не завжди добре уявляють собі структуру самої проблеми, що призводить до плутанини понять і, як наслідок, до неможливості протистояти демагогії і войовничому нецтву та відверто ворожим силам.

Розглядаючи тріаду «наука (фундаментальна наука) — наукова технологія (технологія) — виробництво», можна надати

визначення цих понять і меж між ними. Зокрема, наука — це вид людської діяльності, призначений для виявлення раніше невідомих законів природи і суспільства. Призначення технологій полягає у використанні відомих знань у практичній діяльності людини і суспільства. Виробництво, певно, варто визначити як засіб тиражування досягнень технології.

Цілком очевидно, що межі усередині цієї тріади досить примарні, проте функціональне призначення кожної з її складових цілком зрозуміле. Певне, метод аналогій може прояснити цю суху матерію. Відмінність між наукою і технологією така сама, як і відмінність між розвідкою і головними військовими силами. Історія знає чимало прикладів, коли відсутність розвідки або її погане ведення шкодило армії навіть більше, ніж сам супротивник. Саме тому статuti всіх армій світу вказують на необхідність ведення розвідки безупинно в часі та просторі.

Аналогічними є проблеми при відмінності організаційних принципів існування науки і техніки (технології). Наука має складати безупинне інформаційне зростання рівня і глибини досліджень, а технології — зосереджувати засоби і сили на так званих проривних напрямках. Про це свідчить розподіл сил і засобів, що існував нещодавно у державному забезпеченні науково-технічного прогресу СРСР і США. І там, і тут із ста інновацій в галузі науки і техніки понад 60% припадало на фундаментальні дослідження, більше 20 — на вивчення «проривних» напрямів, близько 13 — на конкретні розробки, призначені для «ринку» і лише 1% виявлявся конкурентоспроможним і давав прибуток, цілком компенсуючи витрати держави на науково-технічний прогрес. Вражає подібність структури витрат і результатів, що підкреслює однакову залежність цих двох країн від сучасного рівня людських знань, а не від політико-економічної системи.

Нааявність в Україні величезного науково-технічного доробку в сфері технологій подвійного використання зумовлює підтримку з боку держави пріоритетних напрямів розвитку науки і техніки, спонукає розробляти довгострокові і середньострокові прогнози його реалізації за допомогою стратегічного й індикативного планування регіональних і міждержавних наукових, науково-технічних і інноваційних програм, захищати вітчизняних виробників інноваційних продуктів від недобросовісної конкуренції на внутрішньому і зовнішньому ринках. Необґрунтова-

на заборона відкритого використання науково-технічних розробок завдає значних збитків економіці України і стримує вирівнювання науково-технологічного рівня оборонного і цивільного виробництва. За інтегрального підходу до управління інформацією змістовний інформаційний ресурс має бути віднесеним до найважливіших стратегічних чинників держави. Організований відповідним чином він стане знаряддям, за допомогою якого можна досягти економічної, технологічної та наукової переваги, що і спостерігається у наявності цілком закономірного зв'язку між обсягами використання змістовної, зокрема науково-технічної, інформації і продуктивністю праці народу і конкурентоспроможністю держави.

У інформаційному суспільстві відбувається трансформація людського часу. Знищується біологічна і соціальна ритмічність, яка пов'язана із зростаючою здатністю контролювати відтворення і середню тривалість життя людини. Відбувається стиснення і скривлення робочого часу: працівник має самостійно керувати робочим часом у гнучкому режимі, а технологія скорочує сукупний робочий час значної частини населення, що поступово призводить до втрати робочим часом свого традиційного значення у життєвому циклі людини та суспільства. Технології дають змогу зробити війни миттєвими, а блискавичне поширення інформації по всій земній кулі і прямі репортажі з місць подій забезпечують темпоральну миттєвість соціальним і культурним подіям. Змішування часів у засобах масової інформації, яке відбувається на одному й тому самому каналі зв'язку за вибором самого глядача, створює такий колаж, в якому часове розгортання перетворюється на плаский горизонт — позачасовість мультимедійного гіпертексту стає визначальною рисою культури.

Стратегія розвитку інформаційного суспільства, підґрунтям якої є інформаційні технології, має стимулюватися активним розвитком обміну змістовним інформаційним ресурсом, що створюється у процесі інтелектуальної діяльності людини, а принцип його «вільного поширення», який до останнього часу застосовувався лише до засобів масової інформації, необхідної перенести на всі види інформації, необхідної для прогресу освіти, науки, культури, миру та демократії.

Сьогодні світові промислові лідери, усвідомлюючи неможливість забезпечити свою технологічну і політичну ізольованість і безпеку, приміряють технологічно, географічно і політично диверсифіковані рішення глобальних науково-технічних проєктів, зокрема протиракетної оборони. На початку січня 2003 року міністр оборони Росії С. С. Іванов зробив сенсаційну заяву: за умов виконання низки вимог Росія може співпрацювати з США у створенні такої системи оборони. Денаціоналізація підходу може означати готовність до можливого розподілу ролей, обов'язків, витрат і, звичайно, дивідендів. Тому, наприклад, Росія розглядає проблеми забезпечення правового захисту результатів науково-дослідних, дослідно-конструкторських і технологічних робіт військового, спеціального і подвійного використання найважливішими на сучасному етапі розвитку своєї економіки. Виходячи з економічної і політичної кон'юнктури, транснаціональні фірми розташовують провідні і високооплачувані професії в Сполучених Штатах, оскільки Америка пропонує їм не тільки найнижчі витрати для одержання провідних технологічних кваліфікацій, а й готову наукову і науково-педагогічну інфраструктуру. Країни, що зможуть запропонувати транснаціональним компаніям подібні умови для науково-технічної еліти і нижчі витрати на розвиток технологічного лідерства, інвестують свої інформаційні ресурси в наукові дослідження і розробки, в освіту й в інфраструктуру телекомунікацій, потрібну для створення робочих місць, зможуть брати участь у цьому глобальному науково-технічному проєкті. Тобто багатство піде до тих країн, які створюють своїм мешканцям не тільки необхідні умови для творчої діяльності, а й керовані організації з кваліфікаціями робітників глобального масштабу.

Таким чином, інформаційні ресурси в сучасних умовах стають системоутворюючим чинником життєдіяльності й розвитку суспільства та держави.

Поняття «ресурси» походить від французького *ressource* — допоміжні засоби (кошти, цінності, запаси, можливості, джерела засобів, прибутків тощо), тобто необхідні елементи для людської діяльності. Коли йдеться про природні ресурси, то широкому загалу цілком зрозуміло, що, перш ніж використувати, треба знайти і видобути. Зрозуміло, що їхні запаси об-

межені й вичерпні. Такого розуміння поки що не виявляється, коли йдеться про інформаційні ресурси.

Дедалі зростаюча роль інформаційних ресурсів потребує теоретичних узагальнень. Слід усвідомити, що інформаційний ресурс — це інформація, яка створена чи виявлена, в установленому порядку зареєстрована, оцінена, яка має визначені закони деградації і оновлення, набуває особливих властивостей, які становлять її сутність і роблять її інформаційним продуктом, з одного боку, і предметом споживання — з іншого. В умовах глобалізації, кризового стану суспільства, об'єктивна оцінка інформаційних ресурсів, у тому числі кількісна, постає як одна із проблем державного рівня, а їх постійний моніторинг, безпека, об'єктивність, вартість становлять потенціал країни.

У процесі діяльності людини матеріальні, енергетичні, інформаційні ресурси виробляються, перетворюються, використовуються тощо. Відтак, від відповіді на питання щодо призначення інформації в процесі людської діяльності безпосередньо залежатиме виявлення і обґрунтування проблем щодо інформаційних ресурсів на новому етапі розвитку людства. На жаль, чинне законодавство України не дає відповіді на це запитання. Водночас стрімкий і глобальний розвиток інформаційних технологій зумовлює збільшення кількості людей, залучених до роботи з інформацією.

За цих умов надзвичайно актуальним є пошук саме системних рішень проблем трансформації політичної, економічної, науково-технічної діяльності відповідно до специфіки перехідного періоду. Серед досліджень останніх років дедалі більше з'являється праць, які визначають необхідність системного підходу до трансформаційних процесів.

У різних країнах у процесі реалізації суспільних інтересів і з огляду на традиції утворення науково-промислових високотехнологічних комплексів мало тривалий період становлення. Інтеграція науки і виробництва не може бути найвищим пріоритетом сама по собі, вона — лише засіб досягнення головної мети, в якій можна вичленили дві складові. По-перше, високотехнологічні виробництва мають задовольняти потреби безпеки своєї країни й одержувати від неї держзамовлення, по-друге, високотехнологічна промисловість має бути спроможною до саморозвитку. Інформація, що не інтегрована в технології, власне некорисна

для виробництва, яку б мінову вартість вона не мала. Сама по собі інформація ні раніше, ні тепер, ні в майбутньому нічого не виробляла, і яким би досконалим не був правовий інститут інтелектуальної власності, реальне становище дослідників і винахідників залишатиметься жалюгідним, якщо не буде попиту на продукт їхньої інтелектуальної діяльності або не матиме правової охорони.

Технічний прогрес породив різноманітні джерела і засоби передавання й одержання інформації. Вражаючий прогрес у галузі інформаційних технологій, якого досягнуто на основі стрімкого розвитку електронно-обчислювальної техніки упродовж останнього півстоліття, породив не тільки в широкого загалу, в суспільній свідомості, а й у багатьох теперішніх державних діячів, деформоване уявлення про сутність інформаційної революції, про її мету і способи розв'язання проблем — у словосполученні «інформаційні технології» найчастіше робиться акцент саме на технології. Тим часом найзначніші досягнення людства XX століття в розвитку науки, техніки і технологій — ядерна програма, успішний вихід у Космос тощо, були зроблені ще до появи сучасних технологій обробки інформації.

Саме запуск перших штучних супутників Землі, тобто поява ракетно-космічних носіїв ядерної зброї, зумовив створення інформаційної мережі Internet, яка 17 травня 1991 року перетворилася на Всесвітнє павутиння (WWW). Міністерство оборони США в умовах «холодної війни» поставило перед американською наукою завдання розробити структуру зв'язку, яка могла б продовжити діяти після ядерного удару, коли більшість комунікацій буде знищена. Основні ідеї лежали на поверхні: потрібна структура, яка не має єдиного головного центру. Тобто потрібно побудувати не дерево зв'язку, а мережу, і побудувати так, щоб пакети даних передавалися з одного вузла на інший, щоб мережа перекидала їх як «гарячу картоплину», і тільки на останньому вузлі — приймачі — пакети збирались у конкретне повідомлення. Тоді був організований ARPA (Pentagon's Advanced Research Project Agency — Передова науково-дослідна асоціація Пентагона) — комітет, який об'єднав потужні наукові сили для роботи над цією проблемою. Перші творчі рішення з'явилися на початку 1960-х років і тоді ж почала створюватись перша глобальна мережа — ARPANET, яка була не зовсім зруч-

ною для використання. Але зручності мереживного обміну виявилися настільки вагомими, що мережа стала стрімко розвиватись і входити в повсякденне життя людства — з'явилася можливість передавання повідомлень і участі в конференціях, перегляд новин і доступ до бібліотек.

Свою другу складову Мережа придбала в CERN (Європейський центр ядерних досліджень, Женева, Швейцарія) в 1989 році. Тут був створений стандарт мови гіпертексту (HTML, текст із вбудованими посилками). Наразі стало зрозуміло, що текст — це ще не все, а до нього можна приєднати зображення та звук. Цей стандарт назвали «Мозаїкою». Були знайдені рішення, які давали змогу зв'язувати вузли Мережі, не дуже напружуючи користувача, приєднавши електронну пошту, і, кінець кінцем, злившись в одну програму, з якою людина має спілкуватися, — наприклад Netscape.

Три перші вузли доступу України до світової мережі з'явилися в 1990 році. Відтоді почалося формування українського сегменту Глобальної мережі, що існує як така після встановлення на центральних комп'ютерах CERN остаточної версії веб-сервера. У 1992 році зареєстрований домен .ua, і сьогодні Україна посідає 28-е місце у Європі та 45-е місце у світі за наданням національних інформаційних ресурсів та використанням світових через мережу. Слід підкреслити, що кількісні відомості про розвиток глобальної інформаційної мережі є вельми умовними, позаяк вона стрімко розвивається і вони швидко змінюються.

Телекомунікаційні технології зв'язали весь світ інформаційними мережами і дають змогу за секунди переводити капітал із однієї економіки в іншу. Заощадження та інвестиції, банки та пенсійні фонди, фондові та валютні біржі в різних країнах, а відповідно і національні економіки стали взаємопов'язаними і взаємозалежними. З'явилася нова економіка, в якій виробництво, споживання і циркуляція товарів і послуг організовуються у глобальному масштабі. Нової структури набувають суспільство, міста, культура і час. Уже в даний час світ став простором безперервних, глобальних, взаємопов'язаних потоків інформації, капіталу, влади, технологій.

Інтернет сприяв лібералізації науки, яка з ієрархічно організованою і національно орієнтованою все більше стає плюралістичною й інтернаціональною, вчені отримали можливість спілку-

ватися між собою й обмінюватися ідеями та інформацією в інтерактивному режимі, що особливо істотно для України, якій у спадщину від тоталітарного минулого дісталися і дотепер ще не зжиті адміністративно-командні традиції управління.

Як зазначається у п. 2 Окінавської хартії глобального інформаційного суспільства, «сутність інформаційних технологій, що стимулюють економічну та соціальну трансформацію суспільства, полягає в її здатності сприяти людям та суспільству у використанні знань та ідей. Інформаційне суспільство, як ми його уявляємо, дає змогу людям ширше використовувати свій потенціал та реалізовувати свої наміри. Для цього ми маємо зробити так, щоб інформаційні технології слугували досягненню взаємодіючих цілей забезпечення сталого економічного розвитку, підвищення добробуту суспільства, стимулювання соціальної злагоди та повної реалізації їх потенціалу в галузі зміцнення демократизації, транспарентного та відповідального управління, міжнародного миру та стабільності. Досягнення цієї мети потребує вироблення ефективних національних та міжнародних стратегій».

В умовах динамічного розвитку світових інформаційних комунікацій технологій, коли вони стають усе більш доступними для кожної людини, а питання створення правового поля, спроможного регламентувати використання Інтернет-технологій, залишається далеким від свого вирішення, найпринциповішою проблемою стає правове регулювання державного управління інформаційними ресурсами, які були створені за рахунок державного бюджету, зусиллями всього українського народу.

Слід зазначити, що комунікаційна система інформаційного століття створює реальну віртуальність — систему за якої зображення на екрані стає не просто образом, який передає досвід, а самим досвідом. Так, під час президентської кампанії 1992 року у США тодішній віце-президент Ден Квейл вирішив виступити захисником традиційних сімейних цінностей і публічно засудив героїню популярної «мильної опери» Мерфи Браун, яка згідно зі сценарієм фільму вирішила завести позашлюбну дитину. Пані Браун одразу ж поклиталася з ним, з'явившись на телеекрані в епізоді, де вона спостерігає інтерв'ю віце-президента, і виступила з різким осудом втручання політиків у своє особисте життя, захищаючи своє право на нову мораль. У результаті серіал

розширив свою аудиторію, а застарілий консерватизм Дена Квейла додав до поразки президента Буша на виборах.

Доступ до глобальних мереж та баз даних, що постійно розширюється, породжує серйозні правові проблеми, до яких, зокрема, належать: конфіденційність інформації та право учасників інформаційного обміну перевіряти відомості, що стосуються цих, безпосередніх, учасників; регламентація змісту інформації, що поширюється через інформаційні магістралі; авторське право, сфера якого потребує багатьох зусиль для поширення правового режиму захисту інтересів власника на цифрове комунікативне середовище, що надзвичайно швидко змінюється, при збереженні доступу до інформації, яка є необхідною для сприяння соціально-економічному розвитку. Той факт, що власне інформаційні технології вже дають змогу частково розв'язати ці проблеми, не змінює суті питання. Водночас слід підкреслити, що відставання країни у сфері створення нових інформаційних технологій може стати незворотним, якщо не буде вжито заходів, спрямованих на виправлення цього становища. Тому потрібні нестандартні рішення, щоб забезпечити прорив у галузі інформаційних технологій для виходу на випереджаючий розвиток нашої країни.

«Інформація» в розвинутих країнах вважається стратегічним ресурсом і є сутнісною складовою цього процесу. Достатньо наголосити, що світовий обсяг виробництва інформаційної техніки й інформаційних продуктів наприкінці 80-х років минулого століття вже перевищив 500 млрд. дол., а саме це виробництво посідає перше місце як за обсягом, так і за кількістю зайнятих у ньому людей³.

Проблемою є саме розуміння, усвідомлення феномену під назвою «інформаційний ресурс». Це поняття, як і поняття «інформація», сприймається нами переважно на інтуїтивному рівні, вони ототожнюються навіть в офіційних документах — як сукупність відомостей, зафіксованих на матеріальних носіях. Водночас інформаційні ресурси держави — це сукупність бібліотечних, у загальному розумінні, фондів доробку інтелектуальної праці людства, поєднаної з інформаційною структурою суспільства, включаючи інформаційно-комунікаційні мережі. Можна стверджувати, що саме розвиток електронної техніки засобів зв'язку зумовив демократизацію нашого суспільства і одночас-

но створив складне інформаційне середовище з численними джерелами одержання інформації і засобами її уявлення та передавання. Управління подібним інформаційним середовищем у національних інтересах очікує свого розв'язання, оскільки являє собою проблему виключної складності.

У провідних країнах світу давно зрозуміли, що інформація перетворилася на реальну силу, стала основним інструментом управління критично важливими структурами суспільства і держави. Багато політичних діячів на конкретних прикладах трансграничних інформаційних операцій, у тому числі безпосередньо військового і терористичного характеру, довели, що нова загроза, або так звана неіснуюча війна, набула реальних обрисів.

Вочевидь, настав час, коли міжнародному співтовариству необхідно реально досягти чіткого розуміння проблеми глобальної взаємозалежності національних інформаційних ресурсів в усій її повноті і комплексності, визнати, що успіх національних зусиль по охороні свого інформаційного ресурсу залежить від рівня захищеності й «неагресивності» інформаційних просторів інших, у тому числі несусідніх держав, із якими їхні інформаційні ресурси об'єктивно пов'язані.

Усвідомлюючи всю серйозність потенційної загрози впливу на свої інформаційні ресурси, провідні країни на національному рівні розпочали реалізацію довгострокових державних програм, спрямованих на забезпечення інформаційної безпеки передусім критично важливих інфраструктур.

Головною метою дослідження, результати якого викладені в монографії, є: системний аналіз політичних, соціально-економічних, організаційно-правових чинників, інституціональної політики формування національних інформаційних ресурсів, виявлення закономірностей, тенденцій, пріоритетних напрямів їх розвитку і використання у різних видах, формах і типах науково-виробничих і господарських структур; дослідження еволюції інформаційної діяльності та розвитку інформаційної індустрії в науково-технічній сфері та обґрунтування умов найбільш ефективного використання інформаційних ресурсів України з урахуванням національних інтересів; розробка основних напрямів стратегії державного управління системою національних інформаційних ресурсів та організаційно-правових засад забезпечен-

ня її реалізації в умовах системної трансформації економіки і суспільства.

Змістовний інформаційний ресурс як зареєстровані відповідним чином відомості про наукові знання і стан соціально-економічного розвитку, що створені або виявлені, мають визначені закономірності деградації та оновлення, і, що інформаційний продукт, який є предметом споживання суспільства, має бути відповідним чином оцінено і захищено.

Проблеми формування, поширення і використання не взагалі інформації, а змістовного інформаційного ресурсу, стали для України сьогодні особливо актуальними тому, що ми маємо долучити їх для зміцнення своєї конкурентоспроможності.

Передусім треба мати «що передавати». А відтак, на першому місці виявляються проблеми формування, поширення і використання саме змістовного інформаційного ресурсу, який є рушійною силою в усіх без винятку сферах суспільно корисної діяльності.

Фундаментальною властивістю змістовного інформаційного ресурсу є обмеженість його розвитку екстенсивним шляхом, тобто простим нарощуванням та інтенсифікацією існуючих інформаційних технологій. Справжній перехід суспільних відносин на новий щабель розвитку відбувається після радикальної розбудови усталених технологій створення, зберігання і споживання інформації — новітніми, що, в свою чергу, потребує застосування нових принципів формування ресурсів змістовної інформації. Для цього потрібні заходи концептуально спрямованої політики держави щодо переведення сучасного інформаційного простору з засад мас-медійного напрямку і проникнення реклами в суспільну свідомість на засади точного механізму управління, автоматизованого посередника кожного з кожним. Звідси: засади управління визначаються через суспільну роль та усвідомлення економічної вагомості інформаційного ресурсу, передусім — за вітчизняним науково-технічним доробком.

Вочевидь, що в Україні сьогодні ще існує пріоритет державних регуляторів, оскільки традиції сформовані в умовах жорсткої державної монополії на ресурси науково-технічної інформації, яка існувала за часів УРСР, особливо у військово-промисловому комплексі, коли підприємства і науково-дослідні установи були позбавлені права прямого виходу на зовнішні ринки.

Політика лібералізації надала їм таке право, але водночас більшість вітчизняних підприємств виявилась не спроможною виробляти науково-технічну продукцію, яка відповідала б світовим взірцям, реалізувати сучасні маркетингові стратегії, використовувати новітні організаційно-фінансові інструменти у своїй діяльності.

Для подальшого розгляду автор обирає термін «*змістовний інформаційний ресурс*» («*змістовні інформаційні ресурси*») — (ЗІР) як ключове поняття замість загального поняття «інформаційний ресурс» (ІР), оскільки останнє є надто широким та має всеосяжний характер, що в багатьох випадках призводить до істотних суперечностей. Поняття ЗІР завжди виокремлювалось у будь-якій інформаційній моделі — від законодавчого до побутового рівня — і передавало розуміння інформації (відомостей, даних) з чітко визначених позицій і напрямів діяльності.

Змістовний інформаційний ресурс у монографії розуміється як систематизоване зібрання (сукупність) синтезованої документованої або публічно оголошеної інформації за її функціональним призначенням про результати вітчизняних і зарубіжних досліджень і розробок та відносно самостійні сфери життя і діяльності людини, суспільства, держави та навколишнього середовища як ресурсу життєдіяльності (функціонування) розвитку біологічних, інженерно-технічних та соціальних систем.

У спрощеному вигляді формування ЗІР — це процеси збирання, накопичення, розвитку і підготовки до використання не будь-якої інформації, а лише тієї її частини, яка має чітке функціональне призначення для сучасного економічного, науково-технологічного, соціокультурного розвитку і прогресу та забезпечення сталого функціонування структур і систем національної безпеки.

Такий підхід дає можливість для визначення пріоритетів у системі національних інформаційних ресурсів, що особливо актуально для України. ЗІР — це ресурс випереджального розвитку, підвищення конкурентоспроможності товарів і послуг, забезпечення рівноправності у відносинах з навколишнім середовищем та цивілізованого інтегрування у світовий інформаційний простір.

Введення поняття *змістовного інформаційного ресурсу* поряд з такими елементами *інформаційної інфраструктури*

(ПФС), як сукупність інформаційних організацій, що фахово займаються опрацюванням ЗІР за видом інформації чи галуззю господарювання і створенням інформаційних продуктів та послуг на підставі такого опрацювання; *інформаційні системи* (ІС) — сукупність інформаційних технологій (техніко-технологічні засоби) разом з традиційними і телекомунікаційними засобами («транспортні магістралі»), — дає змогу розглядати сучасну *інформаційну діяльність* як таку, що оперує в нерозривній єдності своїми складовими — ЗІР, ПФС на засадах відповідного організаційного, нормативно-правового, методичного та кадрового забезпечення. Таке розмежування і чітке організаційно-функціональне визначення складових інформаційної діяльності дає змогу розглядати її на рівні державної політики як інституціональне утворення, серед завдань якого провідне місце належить формуванню *системи національних інформаційних ресурсів* (СНІР) та адекватної організаційної структури для її управління, включаючи створення належних інститутів господарювання — державних і недержавних (які у своїй сукупності формують ринкову інфраструктуру), запровадження відповідних правових форм регулювання їх діяльності.

У монографії поняття «система національних інформаційних ресурсів» розуміється як сукупність систематизованих інформаційних ресурсів суб'єктів інформаційної діяльності України з необхідним довідково-інформаційним фондом і довідково-пошуковим апаратом та правовими, організаційними, методичними, технічними і технологічними механізмами їх формування, розвитку, зберігання, поширення, використання, охорони і захисту.

Ставлення до системи національних інформаційних ресурсів з наукового потенціалу України як до об'єкта дослідження у контексті політики чи економіки і досі є неоднозначним, що особливо відчутно за загальної світової спрямованості до створення інформаційного суспільства. Ця неоднозначність супроводжує СНІР як господарсько-структурну ланку держави ще з 1970-х років, коли вперше виникає потреба в широкомасштабному впровадженні передових досягнень науки і техніки у виробництво. Відтоді державна система науково-технічної інформації (ДСНТІ) розглядалася як «наукова» з позиції економіки чи управління; як «галузева» — з позиції використання наукового

24

потенціалу в господарському комплексі; як «регіональна» — з позиції відомчої структури, до сфери підпорядкування якої належать спеціалізовані інформаційні установи.

Вплив ринкових умов господарювання на використання і міжнародний трансфер науково-технічних досягнень загострив питання технологічної безпеки та захисту науково-технічної інформації. Потреби в науковій і промисловій бізнес-інформації з боку широкого кола підприємств зумовили актуальність надзвичайно цікавого і поки що не вирішеного питання щодо умов доступу до накопичених в Україні результатів фундаментальних та пошукових робіт і включення творчого доробку вчених України в розвиток інноваційного процесу. Актуалізується і проблема відкритості інформації про наукові дослідження та використання їх результатів. Маємо констатувати, що інформація (відомості, дані) отримує свою справжню ринкову вартість, у багатьох галузях суспільно-економічної діяльності.

Розширення політичного і законодавчого простору в частині прав на інтелектуальну власність також вимагає стратегічного поєднання науково-технологічної, інформаційної та інноваційної політики у частині використання ЗІР з наукового потенціалу для вироблення напряду діяльності держави з нарощування факторів конкурентної переваги наукоємних і високотехнологічних виробництв. Держава має взяти на себе відповідальність за державний сектор системи національних інформаційних ресурсів України, маючи за мету підтримку процесу розвитку вітчизняного інформаційного ринку, стратегія розвитку інформаційної діяльності має акцентуватися на проблемах управління, формуванні і розвитку змістовного інформаційного ресурсу, його адекватній організаційній та правовій охороні і захисті.

Оцінка сучасних підходів до стратегічного управління інформаційним ресурсом з наукового потенціалу України свідчить, що вони не дають можливості конструктивно розв'язувати проблеми його ефективного використання, тому що виділяються лише окремі його сторони, без комплексного урахування всіх можливостей і складових. Означений підхід дає змогу використовувати особливості СНІР у спосіб, що сприятиме інформаційному, законодавчому, організаційному аспектам її функціонування, урізноманітнить джерела фінансування в умовах міжнародних ринків. Стратегія управління як основна концеп-

туальна засада дає змогу розглядати СНІР як цілісну систему, визначати з загальносистемних позицій очікуваний результат від використання ЗІР у політиці та економіці країни.

Концепцію функціонування та розвитку СНІР пропонується розглядати як систему принципів, пріоритетних напрямів, шляхів розвитку господарства і наукової сфери, складову концепції економічного та науково-технічного розвитку держави. Для її реалізації необхідно виявити проблемні ситуації, розробити стратегію управління з наголосом на власні фінансові, організаційні, технічні можливості; виявити мету і завдання — основу програмно-цільового управління; знайти форми залучення багатьох учасників до реалізації вироблених стратегій і завдань, тобто, по суті, окреслити шляхи реалізації і розробити механізм управління розвитком СНІР з наукового потенціалу України, запобігаючи нав'язуванню техніцизму в розумінні суті соціального розвитку.

Особливі умови створення та реалізації ЗІР містяться в оригінальності інформаційної новації, яка відтворюється один раз і реалізація якої часто потребує значних витрат (розробка, апробація, перевірка результатів, пошук покупця тощо). Донедавна фінансування таких витрат брала на себе держава. В Україні, як і в інших республіках колишнього СРСР, не було природного попиту на інформацію як чинник, що забезпечував би споживачеві додаткові шанси в конкурентній боротьбі. Можливо тому приватизація, яка відбулася на теренах колишнього СРСР, не враховувала інтелектуальної складової промислових підприємств. Ринок став вимагати перегляду ставлення до інформації з погляду на розвиток її товарності, виявилось, що сукупний капітал приватизованих об'єктів із обладнанням і нерухомістю становить не більше 10 — 15% від тієї суми, ніж якби його продавали із інтелектуальною власністю. Природа ж інформації дає змогу розвиватися на суто комерційних засадах лише невеликій частині інформаційного сектору. Відсутність механізмів координації процесів створення та використання інформаційних ресурсів при включенні їх до господарського обігу веде до істотних економічних втрат.

Характерною особливістю сучасної ситуації щодо зазначеного є дерегуляція ринку телекомунікацій, що дає змогу кабельним, телефонним, стільниковим, супутниковим та іншим

компаніям конкурувати на ринках одна одною, надавати послуги, які раніше були їм заборонені. Глобальна інформаційна мережа, що стала найбільш значним технологічним нововведенням ХХ століття, зумовила неформальні творчі контакти фахівців, стала одним із найбільш діючих чинників розвитку науки і освіти. Це особливо важливо для української науки і промисловості, щоб зайняти відповідне місце у структурі світового ринку високих технологій. Темпи розвитку WWW вражають. Наприклад, за сім років у США вона охопила 30% населення, тоді як телефону на це знадобилось 38 років, а телебаченню — 17. Сучасні телекомунікаційні технології найсуттєвішим чином впливають на обмін інформацією, вимагаючи від учасників обміну (тобто від фізичних осіб до держави) бути особливо пильними щодо охорони своїх інтересів, власності (у тому числі інтелектуальної), дотримання правових норм, щонайменше своєї держави, у процесі обміну (надання, одержання) інформацією. Слід підкреслити, що з розвитком інформатизації всі сфери життя суспільства набувають нових якостей — гнучкості й динамічності.

Таким чином, питання національної безпеки у зазначеному контексті набувають свого практичного значення.

Саме поняття безпеки, за твердженням фахівців, має кілька різновидів. За одними критеріями, безпека містить політичну, економічну, екологічну, військову та інші складові, за другими, більш узагальненими, — безпеку прогресу, соціальну безпеку тощо, за третіми — безпеку особистості, суспільства, держави, системи держав, планетарну безпеку. Пріоритетні загрози для кожної держави зазвичай закріплюються у законі про національну безпеку. Така пріоритетність встановлена Законом України «Про основи національної безпеки України», прийнятим Верховною Радою України 30 липня 2003 року. Національна безпека визначена цим законом як захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечується сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам. Законодавець визначив основні напрями державної політики з питань національної безпеки у сферах: зовнішньополітичній, державної безпеки, війсьній та безпеки державного кордону, внутрішньополітичній, еко-

номічний, науково-технологічний, екологічний, соціальний та гуманітарний, інформаційний. Враховуючи зростання значущості інформаційної складової в усіх сферах життєдіяльності, одним із напрямів державної політики національної безпеки України є інституціоналізація ЗІР, вжиття комплексних заходів щодо захисту та розвитку, зокрема, науково-технологічного потенціалу і створення ефективних механізмів боротьби з несанкціонованим його витоком з України. ЗІР містить документовані або публічно оголошені відомості про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, стає очевидним, що його відповідне використання є, щонайменше, обов'язковою умовою національної безпеки та добробуту держави.

Слід зазначити, що протягом минулих 12 років органи державного управління України були в стані перманентного реформування, кадри фахівців у державних установах постійно змінювалися, а тільки-но накопичений досвід державного управління нерідко втрачався, бо функції, передані іншій структурі, приймали для виконання інші фахівці, зі своїм баченням проблем і досвідом роботи. Потрібен був час для осмислення нових проблем, які постали перед державою, а вони, як відомо, простими не бувають — кожна держава діє в умовах різних обмежень — правових, політичних, ресурсних та ін., і всі держави на міжнародній арені конкурують між собою, а форми цієї конкурентної боротьби можуть бути різними — від інформаційного і економічного втручання у внутрішні справи до прямого військового. Джерела цієї конкурентної боротьби — в боротьбі за життєво важливі ресурси, обстоювання своїх національних інтересів, забезпечення своєї національної безпеки.

У своєму інтерв'ю редакції газети «День» (2.08.01 р.) тодішній Прем'єр-міністр України А. Кінах висловлював таку думку: «...Ми протягом 10 років дуже мало приділяли уваги національним інтересам. Та держава, котра не вміє формулювати й захищати національні інтереси сучасними методами, ніколи не буде ні конкурентоспроможною, ні благополучною».

Тут доречно нагадати дещо з історії Сполучених Штатів Америки, першої президентської республіки і лідируючої держави в сучасному світі. На думку автора, дослідження генезису трансформацій політичних і економічних систем провідних країн світу для українських учених і політичних діячів ще попереду.

Ми лише зазначимо, що першочерговим завданням, яке ставили перед собою «батьки-засновники» США, створюючи Конституційний конвент, було створення ефективної структури державної влади*. Слід визнати, що в Сполучених Штатах Америки реально існує культ Конституції й повага до законів, держави. Водночас, підтримуючи законослухняність і державних мужів, і рядових громадян, державна система цієї країни надає можливість діяти їм у форс-мажорних обставинах поза законом, якщо йдеться про виживання держави, її національну безпеку, без боязні за негативні для себе особисто наслідки.

З цього приводу ще у 1807 р. Дж. Джефферсон висловив таку думку: «Будь-який хороший державний службовець має бути готовим піти на ризик переступити строгу лінію закону, коли цього вимагає виживання держави; виправданням для нього будуть лише його мотиви». Через три роки, у 1810 році, ця думка була ним розвинута і набула форми категоричного ствердження: «Строге дотримання писаних законів, безсумнівно, є одним з найперших обов'язків добропорядного громадянина, але не найважливішим. Закони життєвої необхідності, самовдосконалення, порятунку нашої країни у разі небезпеки є набагато важливішим обов'язком»⁵.

У США протягом майже двох століть стояли і стоять питання захисту національних інтересів, виживання й безпеки держави. Характерно, що, розвиваючи демократичні основи всередині американського суспільства, США як держава на міжнародній арені діють іншими методами. З цього приводу, досліджуючи процес становлення державної влади у США, автори зазначають: «Ще в 1936 р. Верховний суд США виніс рішення у справі «США проти «Кертис Райт експорт корпорейшн», у якому, зокрема, визнавалось, що система «стримань і противаг» не призначена для розв'язання зовнішньополітичних проблем американської держави⁶, і наводять висловлювання відомого політичного діяча і дипломата 1950 — 70-х років Е. Стівенсона щодо діяльності президентів Сполучених Штатів Америки: «Лінкольн і обидва Рузвельти не гралися словами з приводу конституційних тонкощів. Вони діяли»⁷.

Як наприкінці XVIII, так і на початку XXI століття Конституція США залишає за президентом країни неписане право бути активним чи пасивним главою держави — все залежить від

історичних умов, у яких йому доводиться виконувати свою місію — «м'яке» президентське правління в періоди міжнародного замирення, «жорстке» — в періоди криз і міжнародної напруженості. «Усі без винятку державні діячі США, яких американські дослідження відносять до категорії «великих», обіймали президентський пост у періоди серйозних криз в історії країни або світу. Звідси робиться досить поширений у останнє десятиліття висновок, що демократичні принципи здійснення влади у США прийнятні і реальні тільки у безпроблемний час. В умовах же політичних, економічних, воєнних, соціальних криз, що змінюють одна одну — такий ще один висновок — демократія має уступати шлях життєвій необхідності, вимогам оперативності, рішучості і ефективності вжитих на найвищому державному рівні кроків»⁸.

Події у Сполучених Штатах Америки 11 вересня 2001 року, удар терористичного угруповання по національних символах США, загибель тисяч невинних людей, висвітлили нову загрозу людству — тероризм. Цей страшний день назвали «другим Пірл-Харбором Америки», і так само, як рішуче відреагували США на загибель значної частини свого Тихоокеанського флоту від удару авіації Японії 7 грудня 1941 року, так відреагували вони і на терористичний напад 11 вересня 2001 року — проголошено війну на знищення.

Ці події повернули значну частину і політиків, і державних діячів, і пересічних громадян у всіх цивілізованих країнах до суворих реалій життя, сприйняття небезпеки в її нелюдській сутності, поставили питання про незахищеність від нової загрози.

Глобалізація — об'єктивний процес. Оскільки така фундаментальна структура нашого суспільства, як капітал, стала глобальною. Зауважимо: банки, інвестиції, ЗМІ, інформація, наука, технології взаємозв'язані й взаємозалежні. Не всі люди підключені до глобальної мережі, однак всі зазнають її впливу.

Глобальний тероризм — породження і супутник глобалізаційних процесів. Розширення кордонів «вільного світу», створення найкращих політичних, правових і економічних умов для діяльності транснаціональних корпорацій в поєднанні з сучасними інформаційними технологіями водночас забезпечили і спри-

ятливе середовище для діяльності глобальних терористичних угруповань.

Витоки тероризму як такого — у розчаруванні й відчаї багатьох людей у різних країнах. Бідність — лише одна із причин цього явища. Коли цивілізації були ізольовані, ситуація, за якої 25% людей планети контролюють 90% світових багатств, була можлива, проте новітні комунікаційні технології ліквідували цю ізольованість і прискорили процеси глобалізації.

На мою думку, суспільством ще не повною мірою усвідомлено, що 11 вересня 2001 року історія була розколота навпіл — до цієї дати війни велися, як правило, між державами, що мають чітко визначені ознаки: територія — простір, у межах якого поширюється суверенітет держави і на якій органи державної влади здійснюють свої повноваження; населення, що проживає на території держави; публічна влада — здатність, можливість і право визначати суспільну поведінку і діяльність населення, що проживає на її території; податки — загальнообов'язкові й безоплатні платежі, необхідні для забезпечення функціонування органів управління і підтримання життєдіяльності держави; право — система загальнообов'язкових законодавчо закріплених правил поведінки, що є одним з найважливіших засобів управління і починає формуватися з появою держави; армія — збройні сили, що виконують функцію захисту держави від зовнішніх загроз і є необхідним атрибутом будь-якої держави; державний суверенітет — міжнародна правосуб'єктність, здатність держави проводити незалежну зовнішню і внутрішню політику, забезпечувати верховенство державної влади на всій території країни і незалежність держави на міжнародній арені. Іноді виділяють такі додаткові ознаки, як-то єдина державна мова, громадянство, державна символіка, єдина грошова система, єдина інформаційна система, міжнародне визнання. У наш час державі (державам) протистоїть супротивник, який не має ні території, ні визначеного населення, ні публічної влади тощо, залишаються також не відомими і його ресурсні можливості.

Тому постає цілий ряд проблем — від політичних, економічних, військових тощо і до морально-етичних — у засобах ведення збройної боротьби з таким супротивником. У цій боротьбі визнання «перемоги» або «поразки» втрачають загальноприйня-

тий сенс, і, на думку автора, будуть значною мірою визначатися результативністю роботи спецслужб та засобів масової інформації, тобто в інформаційній сфері.

Отже, потенційні можливості *розвитку основних сфер життя* суспільства і відповідних компонентів обороноздатності визначаються станом інформаційних процесів. При цьому зростає і потенційна уразливість суспільних процесів від інформаційного впливу. Вважається⁹, що на зміну небезпеці виникнення ядерної катастрофи може прийти загроза розв'язання війни, що набуде нових форм. Ця боротьба буде спрямована проти країн, що володіють передовими технологіями, з метою створення дезорганізації в їхніх інформаційних структурах і породження економічної катастрофи, а тому збір економічної інформації про конкурентів і захист власних інформаційних ресурсів — головні умови забезпечення безпеки економіки.

У військовій сфері настає постядерний етап розвитку. Ефективність сучасної зброї дедалі більше визначається не стільки вогняною міццю, скільки ступенем інформаційної забезпеченості.

Першою такою війною була 100-годинна війна в Перській затоці в 1991 році. Тоді в іракців була велика армія, оснащена непоганою зброєю, але все сталося досить швидко. Ключовий фактор цього — навіть не електронна точність, а комунікаційна мережа, по якій йде інформація про те, куди цілитися, тобто забезпечується цілевказівка.

Інформатизація управлінських процедур і управління в цілому стало пріоритетним завданням військово-технічної політики. У змісті воєнних дій зросла значущість інформаційно-технічного протиборства. Перевага в ступені поінформованості — неодмінна умова перемоги в повітряному, морському, сухопутному бою, запорука успіху в протиповітряній обороні.

Інша війна точиться в людських мізках. Зброєю в ній є інформаційна політика і глобальні комунікації. Сучасна армія має, з одного боку, рішуче бити технологією, а з іншого — керувати інформацією таким чином, щоб громадська думка не одержала надто багато такої інформації, яка спрямувала б її проти війни: В'єтнамська війна була програна Америкою в університетських колах усередині країни, а не у В'єтнамі.

Зростання ролі інформаційно-технічної боротьби стирає межу між війною і світом. Збройні сили ряду держав перебувають у

постійному інформаційному протиборстві, а військова інформатика й у мирний час вирішує завдання, притаманні війні.

Характеризуючи таким чином проблеми інформатизації й інформаційної безпеки, російські дослідники¹⁰ зазначають, що — у Пентагоні керуються гаслом: «Радіоелектронна війна ніким не оголошується, ніколи не припиняється, ведеться потай і не знає кордонів у просторі й часі». Боротьба за володіння комп'ютерними мережами й обмін «інформаційними ударами» стає дедалі небезпечнішою.

Необхідно зазначити й те, що для участі в цій боротьбі зовсім не потрібно бути «солдатами в шинелях». Це означає, що спеціальні підрозділи інформаційної боротьби можуть виводитися за штатну чисельність регулярної армії, розчинятися в інших державних і недержавних структурах, що створить значні перешкоди для їхньої реальної оцінки, з усіма наслідками цього.

В інформаційному світі «простір місць» заміщується «простором потоків», оскільки суспільство побудовано навколо потоків капіталу, інформації, технологій, організаційної взаємодії, зображень, звуків та символів. Існує, як мінімум, три шари простору потоків. Перший шар — це ланцюг електронних імпульсів (мікроелектроніка, телекомунікації), які створюють матеріальну основу найважливіших процесів суспільства — технологічна інфраструктура визначає новий простір так само, як залізниця — індустріальну економіку. Другий — це вузли і комунікаційні центри, що координують взаємодію елементів, інтегрованих у мережі. Третій шар простору належить до просторової організації домінуючих менеджерських еліт.

Отже, інформаційна безпека на початку ХХІ століття виходить на перше місце в системі національної безпеки і вимагає проведення єдиної державної політики в цій пріоритетній сфері. А оскільки будь-яка політика в правовій державі повинна мати правове підґрунтя, то виключно важливо визначити її правові основи. Поки ж, на жаль, розвиток суспільних відносин у цій сфері істотно випереджає розвиток права з цих питань, на чому ми зупинимось в процесі подальшого розгляду проблеми.

Науково-технічний потенціал держави багато в чому залежить від інформаційного забезпечення праці вчених, інженерів, наявності систем автоматизації проектування (САПР), автоматизованих систем наукових досліджень (АСНД), засобів прове-

дення обчислювальних експериментів, телеконференцій — низький рівень цього забезпечення не дає змоги проводити дослідження на передових рубежах науки і техніки і є однією з основних причин «витоку мізків» із країни.

Тому автор, усвідомлюючи актуальність для України проблем ефективного використання змістовних інформаційних ресурсів, насамперед з науково-технічного доробку, що в свою чергу неможливо без розв'язання проблем інформаційної безпеки, переходить до розгляду основних проблем.

РОЗДІЛ 1

КОНЦЕПТУАЛЬНІ ЗАСАДИ ДЕРЖАВНОГО УПРАВЛІННЯ НАЦІОНАЛЬНИМ НАУКОВО- ТЕХНІЧНИМ РЕСУРСОМ

1.1. КОНЦЕПТ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ В СУЧАСНОМУ СВІТІ

До ХХІ століття світова політика формувалася як складне багатовимірне утворення, основою якого є принципи культурного різноманіття, ідейного плюралізму, фінансової глобалізації. Геополітична карта світу сьогодні структурується не через контрасти чи протиставлення системних ідеологій, а через взаємовплив і взаємопроникнення державних інтересів. Сьогодні перед кожною державою постає завдання вироблення такої зовнішньо-і внутрішньополітичної стратегії, яка повною мірою відповідає вимогам сучасного контексту глобалізації й багатополюсності.

Слід зауважити, що тільки мобілізоване, активне, добре поінформоване громадянське суспільство може протистояти спокусам гегемонії суперсили. Нині ми входимо в дуже нетривкий світ, де погано поінформовані й заангажовані політики, якими маніпулюють екстремістські ідеологи у Вашингтоні, можуть вирішувати питання життя й смерті людей на усій планеті. Природно, що Європейський Союз, Китай і Росія мають діяти спільно на противагу унілатеризму США.

У сучасному глобальному світі більшість людей, працюючи або розважаючись, веде дуже локальний спосіб життя. При цьому люди схильні гуртуватися навколо первинних джерел ідентичності — релігійних, етнічних, територіальних, національних — особливо в часи неконтрольованих і безладних змін.

Відмітна соціальна й політична тенденція 1990-х років минулого століття — це побудова соціальної інфраструктури й політики навколо первинних ідентичностей. Так, захист суб'єктивного миру в особистості заміняє ідею класової боротьби в культурі. Однак побоювання, що ісламський і християнський світи можуть повністю відокремитися один від одного — дуже спрощене розуміння проблеми. Більшість людей у християнському світі не ідентифікує себе насамперед із релігією. У Європі релігія — вторинний чинник. Справді, у мусульманському, арабському світі ЛЮДИ нині вибудовують свою ідентичність, захищаючись таким чином від впливу західної ідеології, протидіючи їй, у тому числі у формі терористичних актів. Для викорінювання джерел тероризму потрібен саморозвиток, культурний діалог між християнською і мусульманською Цивілізацією.

Сучасні програмно-апаратні засоби інформаційних технологій — них процесів значно розширили можливості активного залучення до інформаційного обміну і відносин великої кількості людей, громадських організацій, наукових установ, промислових підприємств, державних інституцій, і тим самим прискорили демократичні зміни в країні, що в свою чергу дає можливість Президентові України орієнтувати наше суспільство на підвищення конкурентоспроможності економіки України на світових ринках.

Не можна вважати, що нові українські еліти склалися спонтанно, однак вони ще не відчувають повною мірою відповідальності за свої висловлювання і дії щодо розбудови нашої держави в глобальному інформаційному середовищі.

Минулі парламентські вибори і кадрові перестановки, що відбулися після них, зафіксували прихід до влади в Україні власників і менеджерів високоприбуткових кампаній. Застосувавши випробувані прийоми агресивного захоплення ринків, вони отримали владу, і є сподівання, що використають її на користь народу України, розвитку вітчизняних високотехнологічних виробництв. Перед Верховною Радою України четвертого скликання стоїть завдання адекватно оцінити проблеми в інформаційній сфері та надати юридичне тлумачення понятійно-категоріального апарату інформаційної сфери на рівні законодавства. Зокрема, це стосується таких визначальних для регулю-

вання інформаційних правовідносин понять, як: «інформація», «інформаційний ресурс», «правовий режим інформації», «інформаційна безпека», «інформаційний суверенітет», «національний інформаційний простір» тощо, які є виключно важливими для створення в Україні умов для обміну ідеями та інформацією, що є запорукою її інноваційного розвитку.

Структура і функціональне наповнення складових системи державного управління національними інформаційними ресурсами безпосередньо залежатимуть від мети держави, сформульованої в Основному Законі — Конституції України і розвинутої щодо інформаційної сфери в Концепції державної інформаційної політики. Формулювання мети діяльності (функціонування) будь-якої системи завжди передують перетворенню її на дії, для практичної реалізації визначаються функції структурних елементів системи, забезпечуються їх легітимність і ресурси для функціонування системи.

У процесі розроблення концепції перед вітчизняними фахівцями стоїть складне завдання — за роки незалежності напрацьовано значний масив правових актів у галузі інформаційного законодавства, а концепція має з'явитися тільки тепер. Якою мірою вона має враховувати нині діючі правові документи і як вирішувати існуючі в чинному інформаційному законодавстві неузгодженості та нерозв'язані проблеми?

На нашу думку, перш ніж відповісти на ці непрості запитання, слід визначитися, що маємо на увазі, коли йдеться про інформаційну політику і як вона має впливати не тільки на найважливіші сфери суспільного буття в країні, а й забезпечити об'єктивне уявлення про Україну за її кордонами, у світі?

Відповіді на ці запитання лежать поза площиною відомчих, фрагментарних міркувань і вимагають від держави системного підходу до проблеми.

Так само, як створення воєнної організації держави є справою всієї держави — її вищих державних органів, наукового, технологічного і виробничого комплексу, систем освіти і охорони здоров'я тощо, а не тільки Міністерства оборони, так і побудова основ інформаційного суспільства потребує системного підходу з боку держави за активної участі суспільства у розв'язанні багатогранних проблем інформаційної сфери.

Зауважимо, що спрямованість провідних країн світу на побудову інформаційних суспільств у своїй основі має суто прагматичні цілі, а модель становлення інформаційного суспільства у кожній країні має свою національну специфіку.

На сучасному етапі розвитку цивілізації, який, за оцінками фахівців, триватиме у США до 2020 року, в розвинутих країнах Європи до 2030 — 2040 років¹¹, найрозвинутіші регіони світу здійснять перехід від індустріального до інформаційного суспільства — що зумовлено тим, що в людства немає іншої альтернативи, яка надавала б йому змогу зберегтися як біологічного виду і забезпечити при цьому можливості для подальшого прогресу суспільства.

Єдиним способом радикального підвищення інтелекту людства до рівня, достатнього для вирішення стратегічного завдання виживання і розвитку цивілізації на гуманістичній основі, відомий людству і здійснюваний практично, є інформатизація. Для розуміння наших подальших міркувань дуже важливі ці два положення, а саме: мета переходу до інформаційного суспільства — по-перше, збереження людства як біологічного виду і забезпечення можливостей для подальшого розвитку суспільства; по-друге, спосіб досягнення мети — інформатизація.

Усвідомлення цих положень дасть правильну відповідь на запитання: що має становити основний зміст державної інформаційної політики? Ми акцентуємо увагу на цьому, оскільки і запропонований Держкомінформполітики для розгляду у 2001 році проект Інформаційного кодексу України, і поданий у липні 2002 року для громадського обговорення проект Концепції національної інформаційної політики несуть на собі відбиток суто відомого розуміння проблем, які існують в інформаційній сфері.

Слід зауважити, що інформатизація — це глобальний процес, який супроводжується кардинальною зміною структури і характеру світового економічного і соціального розвитку, переходом до наукоємного виробництва, нових видів інформаційного обміну, і впливає на більшість сфер суспільної діяльності, змінюючи характер світового розвитку, соціально-економічні відносини в ньому, рівень і якість життя всіх членів суспільства.

Національні моделі становлення інформаційного суспільства, узагальнені стратегії та програми інформатизації індустріально

розвинутих країн, їхня інформаційна політика досить ґрунтовно розглянуті¹².

Так, американсько-англійська модель, запропонована у 1993 році як президентська стратегія США, покладена в основу всіх існуючих моделей формування інформаційного суспільства. План дій адміністрації США в сфері Національної інформаційної інфраструктури (The National Information Infrastructure: Agenda for action, 1993) став найважливішою ініціативою адміністрації Клінтона — Гора¹³.

Позицію Конгресу США щодо національної інформаційної політики викладено в доповіді Ф. Вайнгартена «Удосконалення федеральної інформаційної політики: погляд Конгресу» (1996 р.), де зазначається, що Сполучені Штати сприймають інформаційні проблеми як політичні чинники для прийняття рішень, що невід'ємні від глобальних проблем американського суспільства. Інформація є одним з основних ресурсів держави, а системи, покладені в основу її створення, обробки і поширення, сприяють прогресивному розвитку і становлять основні соціальні інфраструктури суспільства. Інформаційна індустрія тлумачиться як головний стратегічний чинник конкуренції та провідний сектор економіки країни.

Інформаційна політика охоплює широке коло урядових заходів: спрямованих на створення інформаційних технологій і управління ними; пов'язаних з потоками інформації; пов'язаних із впливом інформаційних технологій і потоків інформації на конкретні установи чи сферу суспільної діяльності.

Пріоритетами національної інформаційної політики США визначені: підтримка досліджень і розробок у галузі інформації і комунікації; вплив на їхнє спрямування та заохочення до поширення технічних знань і можливостей в економіці; сприяння обміну технологіями між лабораторіями та фірмами, запровадження нововведень на ринках; побудова та вдосконалення інформаційної інфраструктури, контроль за її діяльністю, побудова глобальних систем комунікації і дослідження впливу систем на міжнародні, національні і приватні пріоритети; збереження порушеної новими технологіями рівноваги між чотирма основними інформаційними цінностями: конфіденційністю інформації, інформацією як суспільним благом, інформацією як товаром, інформацією як невіддільним компонентом існування держави (необ-

хідне відновлення цієї рівноваги і встановлення нових засобів контролю для нових інформаційних відносин); недоторканність приватного життя, конфіденційність інформації приватного характеру на різних рівнях та в різних сферах державного управління і в приватному секторі; формування урядової політики в галузі інформації і комунікації.

Інформаційна політика Канади спрямована на забезпечення лідерства держави у запровадженні і використанні комунікаційних систем та електронної інформації, створення так званого електронного уряду Канади, для забезпечення прозорості діяльності владних структур та доступу громадськості до урядових департаментів електронними засобами. Національна програма побудови інформаційного суспільства та нових технологій (1996 рік) (Building the Information Society: Moving Canada into the 21-st Century. Ministry of Supply and Services, 1996) включає такі стратегічні елементи, як побудова інформаційних супермагістралей, орієнтованих на суспільні інтереси та ринковий попит; вибір (створення) відповідального уряду, який виступає каталізатором розвитку інформаційного суспільства та нових технологій; трансформація національної економіки, стимулювання та заохочення транснаціональних проектів у фінансуванні інформаційної магістралі; збалансований прогрес між: ринками і соціальною сферою суспільства.

У англійській моделі роль держави обмежується створенням умов для ринкової конкуренції в інформаційній сфері; стратегія розвитку суспільства визначається як приватна ініціатива, лібералізація ринку телекомунікацій, створення мереж та інформаційних супермагістралей, захист нових структур на інформаційних ринках.

Мета інформаційної стратегії Великої Британії — вдосконалення умов конкуренції на інформаційному ринку, зростання ефективності інформаційних послуг і впровадження інформаційних технологій у сферу державного управління. Інформаційна політика держави гарантується відповідними правовими нормами щодо свободи інформаційної економіки та захисту національних інтересів країни в регіоні та на міжнародних ринках. Характерною рисою інформаційної політики Великої Британії є створення регіональних мереж і супермагістралей для оптимізації та підвищення ефективності міжрегіонального та міжнародного

науково-технічного співробітництва. Так, впроваджуються інноваційні технологічні проекти («Tanet», «SuperTanet», 2001 р.), які передбачають використання нових технологій, розширення доступу до інформаційних ресурсів у різних електронних мережах, підвищення ефективності наукових досліджень, наукового обміну та співробітництва на міжнародному, регіональному та національному рівнях, розвиток потенціалу мережі.

Слід зауважити, що специфічною рисою англо-американської моделі інформаційного суспільства є вплив чинного законодавства на розвиток перспективних галузей економіки, політики, зокрема трудового, авторського права, права інтелектуальної власності, соціального захисту населення¹⁴.

Інформаційна політика Федерального Уряду Німеччини включає концепцію вільного транскордонного обміну інформацією, вільного вираження поглядів, розвитку комунікаційних та інформаційних мереж і систем, вільної конкуренції в інформаційній сфері, створення відповідно до нових політичних, економічних та інформаційних змін у німецькому суспільстві норм і принципів правового регулювання інформаційної діяльності. Сучасна стратегія національної інформаційної політики ФРН («Info-2000: German's way to the Information Society», 1996) визнає головними напрямками: становлення інформаційного суспільства в Німеччині; створення інформаційної економіки; розвиток інформаційних супермагістралей, інформатизацію державного управління; лібералізацію телекомунікацій, підтримку національних виробників електронної продукції, одночасний розвиток державного і приватного інформаційного бізнесу; активізацію земельної інформаційної політики з розширенням прав земельних урядів щодо обігу інформації та діяльності суб'єктів інформаційних відносин у федеральних землях і посилення відповідальності земель і контролю за змістом інформації. Закон «Про Інтернет» (1997 рік) визначив, зокрема, межі сприяння розвитку засобів комунікації та національних мереж і систем у країнах Центральної і Східної Європи. Інформаційна політика ФРН за цим напрямом спрямована на реформування державного управління в цих країнах, забезпечення їхньої участі у транскордонному вільному обміні інформацією, пропаганду ідеалів європейського демократизму, створення відповідної правової бази, технічного оснащення інформаційного сектору та підготовку

висококваліфікованих фахівців у Німеччині для національних та приватних корпорацій, установ, фондів, спілок.

Мета інформаційної політики Франції — становлення інформаційного суспільства, розвиток інформаційних супермагістралей (із забезпеченням франкомовності мереж), електронного ринку і банківської сфери, лібералізація комунікацій, оновлення інформаційного законодавства, стимулювання наукових досліджень у галузі інформаційного бізнесу, створення систем безпечної інформації, запобігання комп'ютерним злочинам. Програма інформаційного суспільства Франції (1998 рік) визначає пріоритетні напрями співробітництва з цього питання в межах компетенції міністерства зовнішньої політики. Формування нових норм і принципів правового регулювання інформаційної діяльності дасть можливість, як зауважено у цій програмі, забезпечити функціонування єдиного ринку товарів та послуг в інформаційному суспільстві. Пріоритетними стратегіями визнано культурну і мовну різноманітність (у мережі Інтернет, Європейських комунікаційних мережах і системах); координацію міжнародного співробітництва у боротьбі проти нових форм злочинності в інформаційній сфері, підвищення ефективності процедури взаємодопомоги в правоохоронній та судовій сферах; створення нових міжнародних договорів та угод про комп'ютерні злочини; вдосконалення систем електронних платежів (особливо електронного підпису), охорони прав споживачів, інтелектуальної власності та приватного життя, розробку регуляторних механізмів для країн європейського ринку.

Інформаційна політика країн Бенілюксу (Бельгія, Нідерланди, Люксембург) формується на засадах концепції становлення інформаційного суспільства під егідою ЄС.

Цей вплив помітний у програмах Федерального уряду Бельгії щодо створення умов для розвитку інформаційної економіки, введення нових компонентів зовнішньої політики, зміні законодавства, процесах конвергенції і лібералізації комунікацій, трансформації муніципального управління. «Федеральна ініціатива щодо становлення інформаційного суспільства» (1994 рік) спрямована на підвищення соціальної активності бельгійського суспільства, реалізацію творчих можливостей кожного індивіда, розвиток інновацій та інтелектуального потенціалу країни. «Плані

дій щодо провідної ролі Бельгії в інформаційному суспільстві» (1998 рік) включає напрями: створення системи електронного уряду; забезпечення гарантій широкого доступу до сучасних інформаційних мереж і недопущення дискримінації за інформаційною ознакою; побудову національної системи телекомунікацій (Бельгійської інформаційної супермагістралі); заохочення досліджень та інновацій для інформаційної економіки; розробка гнучких принципів регулювання інформаційної сфери. Стратегія прискореного безінфляційного економічного зростання передбачає залучення корпоративних інвестицій у дослідження нових інформаційних технологій та Інтернет і впровадження розробок в економіку Бельгії.

Програма уряду Королівства Нідерланди — «Біла книга модернізованого уряду інформаційної доби» (1996 — 2005 роки) передбачає провідну роль держави в радикальній трансформації голландського суспільства. Основні напрями реалізації інформаційної політики стосуються інвестування досліджень та виробництво продуктів в інформаційній сфері (Голландія займає 6-е місце у світі й 3-є місце у США як зарубіжний інвестор); розвитку електронної комерції і лідерства країни в глобальній комунікації; створення електронного уряду і ефективної системи державного і муніципального управління; здійснення спеціальних програм захисту населення від безробіття; запровадження новачій в загальну інфраструктуру; впровадження інформаційних технологій в освітню і культурну сфери.

Інформаційна політика Люксембургу, де розташовані резиденції Європейського інвестиційного банку, Міжнародний фінансовий центр, організації та установи західноєвропейських країн, полягає у впровадженні рішень та програм ЄС, в активному інвестуванні інформаційного сектору, в стимулюванні наукових досліджень у галузі нових технологій, розвитку електронної комерції та програм широкого доступу до інформаційних послуг за допомогою Інтернет.

Попри національну специфіку, політичні пріоритети, економічні можливості і громадську думку щодо інформаційних процесів, скандинавські країни мають такі спільні цілі і напрями здійснення інформаційної політики, як:

— впровадження нових технологій у систему державного

управління і ефективне здійснення політичної влади — забезпечення доступу широкої громадськості до урядової інформації, розвиток мережі «інфоцентрів» для задоволення потреб населення, створення державних мереж управління по вертикалі і горизонталі влади;

— розвиток інформаційної економіки; підтримка інформаційного бізнесу, національних виробників інфопродукції, створення інформаційно-довідкових корпорацій з тематичними базами даних про інформаційні ТНК, компанії, фірми; залучення інвестицій у національні інформаційні проекти;

— забезпечення соціальної сфери комп'ютерними технологіями; організація електронних бібліотек, доступ до інформації в мережах і системах для соціально незахищених верств населення — молоді, інвалідів, малозабезпечених; створення громадського радіомовлення.

Концепція інформаційної політики передбачає також впровадження правових, етичних та освітніх принципів комунікацій та інформації в усі сфери життєдіяльності суспільства відповідно до національних інтересів.

Данія — розвиток сфери електронних послуг та електронних платежів, створення інформаційної супермагістралі, поширення інформаційної продукції «Tele Denmark» на ринки Німеччини і Великої Британії.

Норвегія — розвиток універсальних і спеціалізованих інформаційних мереж, впровадження технологій у політичне життя і волевиявлення громадян (під час виборів).

Швеція — гармонізація цілей національної та європейської інформаційної політики, створення інформаційного законодавства, технічних стандартів; розвиток інформаційної індустрії і бізнесу на базі концерну «Ericsson», інтенсивний розвиток мультимедіа.

Фінляндія — створення і розвиток інформаційних магістралей, інтенсифікація інформаційної економіки, інформаційного бізнесу, проект Nokia, впровадження нових технологій у державне управління, забезпечення доступу громадськості до Інтернет, правові та етичні засади інформаційного суспільства. У 1995 році в Фінляндії прийнято програму (національну стратегію), яка дістала назву «Фінський шлях в інформа-

ційне суспільство» (Finland's Way to the information society. The national strategy)¹⁵.

Характерними рисами європейської моделі інформаційного суспільства є варіативність і політична спрямованість програм побудови такого суспільства для різних країн, зумовлених новою європейською геополітикою, становленням інформаційної (інтелектуальної) економіки, різними можливостями постіндустріального розвитку. Політична стратегія ЄС забезпечує провідну роль держави в перехідний період, яка виступає гарантом інтересів суспільства в умовах становлення інформаційної економіки та розширення сфери інформаційних послуг на всіх рівнях життєдіяльності держави. Відмінність європейської моделі від американської полягає в створенні інформаційного законодавства, адекватної законодавчої бази, яка враховує як національні, так і міжнародні принципи регулювання інформаційних відносин, вважається основним чинником зростання прибутку країни і потенціалу інформаційно-комунікаційних технологій¹⁶.

У 1989 році в колишньому СРСР була розроблена і прийнята Концепція інформатизації радянського суспільства, державної політики інформатизації Російської Федерації яка має відповідну нормативно-правову базу і реалізується органами державної влади за такими напрямками, як:

— заохочення конкуренції: боротьба з монополізмом, контроль за концентрацією власності в засобах масової інформації (ЗМІ);

— юридичне і технологічне забезпечення права і технічних можливостей на доступ до інформації та інформаційних ресурсів всього населення країни;

— реалізація концепції універсального доступу, який передбачає гарантії держави на набір послуг (телефон, електронна пошта, мультимедійна освіта), які постійно розширюються;

— додержання свободи слова незалежно від технологічного середовища поширення інформації;

— захист інтересів національних меншин, підростаючого покоління в інформаційній сфері, особливо у сфері моральності;

— переорієнтування системи освіти з урахуванням вимог інформаційного суспільства, впровадження дистанційного навчання;

— зміцнення національної культури, мови, протистояння

культурній експансії інших країн, переведення у цифрову форму представлення художньої та наукової спадщини;

- широке використання телемедицини для забезпечення послуг для населення віддалених регіонів;

- забезпечення інформаційної безпеки особи і суспільства, включаючи боротьбу з комп'ютерними і високотехнологічними злочинами; охорона інтелектуальної власності; контроль за ефективністю використання сучасних інформаційних і телекомунікаційних технологій у державних установах;

- цілеспрямоване використання інформаційних і телекомунікаційних технологій для формування більш відкритої, демократичної держави, розширення діалогу з громадянами;

- розробка концепцій, стратегій і програм переходу країни та її регіонів до інформаційного суспільства в процесі інформатизації;

- організація проведення наукових досліджень фундаментальних проблем інформатики, які можуть привести до принципово нових рішень, до прориву в галузі створення нових інформаційних засобів і технологій, різкого підвищення ефективності та розширення сфер їх застосування;

- проведення фундаментальних і прикладних досліджень з проблем інформатизації та наукове супроводження програм інформатизації.

Російські фахівці слушно вважають, що в процесі переходу до інформаційного суспільства держава має взяти на себе роль каталізатора змін, що здійснюються, координатора дій різних суб'єктів суспільства, сформувати таку правову і нормативну базу, яка спрямує їх у русло, сприятливе для розвитку суспільства і особистості. При цьому найважливішою умовою розробки і реалізації науково обгрунтованої державної політики інформатизації є науково-методологічне супроводження цього процесу, а також планів, проектів і програм інформатизації на всіх рівнях та всіх етапах її здійснення, починаючи від розробки і наукового обгрунтування політики і стратегії інформатизації, і закінчуючи аналізом результатів і наслідків інформатизації з підготовкою рекомендацій з ефективного використання цих результатів і ліквідації або компенсації її негативних наслідків¹⁷.

Інформатизація є наукоємною сферою суспільної діяльності,

яка вимагає високих технологій і великих витрат. Цей складний соціально-техногенний процес стосується багатьох суб'єктів — підприємств, установ, організацій і практично всього населення країни. Основою цього процесу є масове застосування інформаційних засобів і технологій, підкреслимо, в усіх сферах суспільної діяльності для радикального поліпшення умов праці та якості життя населення, значного підвищення ефективності всіх видів виробництва.

Тому державою мають бути ліквідовані відомчі бар'єри, створені умови для загальної заінтересованості в інформатизації як ефективному засобі прискорення процесу досягнення мети соціально-економічного розвитку, забезпечені координація і регулювання, зауважимо, збалансованого розвитку окремих складових процесу переходу до інформаційного суспільства.

Основним підсумком інформатизації вбачається забезпечення умов для вільного і своєчасного доступу населення до світових інформаційних ресурсів, формування потреби і усвідомлення необхідності їх використання в процесі своєї діяльності у кожного громадянина.

Аналізуючи існуючі у світі програми, проекти, стратегії, можна виявити такі інваріантні властивості, які складають ядро будь-якої концепції переходу до інформаційного суспільства:

- використання комплексного підходу, заснованого на додержанні балансу інтересів держави, суспільства, бізнесових кіл, особи, а враховуючи, що формування інформаційного суспільства відбувається під впливом таких факторів, як поява нового покоління інформаційних і телекомунікаційних технологій, глобалізація ринків, конкуренція в країні і на міжнародній арені, для гармонійного входження в інформаційне суспільство необхідні координуючі та спрямовуючі зусилля з боку держави як органу, здатного виражати і захищати інтереси всього суспільства;

- гуманістична спрямованість концепції має виключити ситуації, за яких будь-хто буде «виключений» з інформаційного суспільства, а суспільство буде розподілене на тих, хто має інформацію, та тих, хто її немає;

- економіка інформаційного суспільства заснована на знаннях, тому освіта і навчання мають бути доступні кожному упро-

довж усього життєвого шляху, а системи освіти і професійної перепідготовки мають забезпечити виконання цих умов, тобто інформаційне суспільство — це суспільство безперервного навчання.

Якщо побудувати дерево цілей інформатизації, то можна виділити її *перший рівень* — генеральну мету — забезпечення необхідного рівня поінформованості населення, що визначається повнотою, точністю, достовірністю і своєчасністю одержання інформації, необхідної людині для виконання нею суспільно значущих видів діяльності, у свою чергу, вимоги до рівня поінформованості людини впливають з цілей соціально-економічного розвитку країни, і *другий рівень* — основні складові генеральної мети, якими є: *інформаційне забезпечення всіх видів суспільно значущої діяльності людини*, що включає пошук, збирання, зберігання, накопичення, обробку і представлення! інформації у формі, зручній для застосування в ході практичної діяльності людини, а основу інформаційного забезпечення! складають фонд (банк, база даних) інформаційних ресурсів у відповідній формі представлення і сукупність методів і засобів організації, підтримання і використання цього фонду, тобто фактично відома фахівцям з обробки інформації в автоматизованих системах виробництва система ведення інформаційних масивів; *інформаційне забезпечення активного відпочинку та дозвілля населення*, яка забезпечувала б людині можливості для дистанційного доступу за допомогою сучасних інформаційних технологій до скарбниці світової культури та створення індустрії розваг та її використання; *формування і розвиток інформаційних потреб населення* передбачає створення таких соціальних і економічних умов, за яких у людини в процесі її діяльності виникає потреба та інтерес до нарощування рівня своєї поінформованості, в іншому випадку інформатизація втрачає сенс; *доброту умов і підтримання умов* — політичних, соціально-економічних, наукових, правових, організаційних і організаційно-технічних, які забезпечили б здійснення інформатизації, процесів контролю за її ходом і управління інформатизацією.

Отже, інформатизація — це процес створення, розвитку та масового застосування новітніх інформаційних засобів та технологій, які забезпечують досягнення і підтримання рівня по-

інформованості всього населення країни, необхідного і достатнього для кардинального поліпшення умов праці, підвищення її ефективності та якості життя кожної людини.

Вважається, що в підсумку інформатизація дасть змогу вирішити низку питань у політичному, соціальному, економічному та управлінському аспектах.

У *політичному аспекті* передбачається:

- підвищити політичну і суспільну активність населення шляхом забезпечення доступу до інформації, яка надасть можливість: об'єктивно оцінити політичні, економічні і соціальні процеси в регіоні, країні, у світі; виразити і довести думку кожної людини до відповідних політичних інституцій та громадських організацій;

- сприяти зближенню та консолідації людей, зростанню взаємодовіри, встановленню та підтриманню дружніх міжнаціональних та інших соціальних відносин;

- сприяти розвитку демократії та гласності, прогресивним перетворенням, розвитку та зміцненню політичних інституцій та громадських організацій, які здійснюють та підтримують такі перетворення.

У *соціальному аспекті* інформатизація дасть змогу :

- сприяти здійсненню принципів соціальної справедливості при розв'язанні соціальних проблем;

- сприяти зміцненню здоров'я та підвищенню творчої активності людей;

- підвищити рівень і якість освіти, значно прискорити рух уперед у різних галузях знань;

- підвищити рівень культури суспільства, надати кожній людині право на засвоєння скарбів світової культури;

- створити необхідні умови для інтелектуальної, творчої, високопродуктивної та науково організованої праці, скорочення та повного витіснення важкої та монотонної фізичної праці, розкриття творчих здібностей людини;

- розвинути та надати нові форми дозвілля та відпочинку населенню;

- здійснити безперервний моніторинг за станом довкілля з метою запобігання негативним впливам людини на природу і вжиття дієвих заходів для захисту людини від природних явищ,

які завдають шкоди її здоров'ю, матеріальному та соціальному становищу;

- прогнозувати шляхом моделювання соціальні, економічні та екологічні наслідки масштабних проектів до їх практичної реалізації;

- сприяти соціальній та правовій захищеності населення, реалізація всього комплексу прав (соціальних, економічних, громадянських, політичних, культурних) громадянина кожною людиною, демократизації та гуманізації суспільства, побудові правової держави;

- усунути з процесу трудової діяльності ряд рутинних операцій та вивільнити час для творчості, підвищуючи тим самим ефективність та привабливість праці для значної частини населення;

- підвищити якість життя населення шляхом підвищення комфортності побутових умов, забезпечення можливості оздоровлення довкілля та ведення населенням здорового способу життя, створення умов для самоосвіти і навчання, проведення вільного часу з користю не тільки для себе, а й для суспільства;

- створити додаткові передумови для успішної боротьби з такими асоціальними явищами, як алкоголізм, наркоманія, токсикоманія, куріння, допомогти відволікти молодь від участі в різних протиправних діяннях, що розширить коло засобів для успішної боротьби із злочинністю.

В економічному і управлінському аспектах інформатизація має:

- привести обсяги і структуру виготовлення продукції у відповідність до потреб суспільства;

- забезпечити пріоритетний розвиток наукоємних галузей! виробництва, впровадження ресурсо- і енергозберігаючих технологій;

- забезпечити прискорення науково-технічного прогресу, скорочення строків і підвищення рівня наукових досліджень, проектно-конструкторських робіт і технологічної підготовки виробництва;

- інтенсифікувати виробництво на основі широкомасштабного використання вбудованих у технологічне обладнання за-

собів сучасної інформаційної техніки, інтеграції автоматизованих систем управління і обробки даних на всіх стадіях життєвого циклу створюваних виробів;

- вдосконалювати внутрішньо- та міжрегіональні і галузеві зв'язки;

- створити ефективне інформаційне забезпечення для органів державного, місцевого і регіонального управління;

- підвищити ефективність управління соціально-економічним розвитком шляхом підвищення якості прийнятих рішень у всіх сферах діяльності, забезпечення можливості залучення до вироблення рішень широкого кола фахівців, попереднього ознайомлення населення зі станом проблем та альтернативними варіантами їх розв'язання, ефективного контролю за здійсненням і наслідками виконання прийнятих рішень, своєчасного ознайомлення населення про результати контролю і, в разі необхідності, оперативного коригування виконуваних рішень.

Такими з позицій сучасної науки можуть бути прямі результати інформатизації¹⁸.

Отже, концепт інформаційної політики в сучасному світі дедалі більше розширюється від поняття політики пропаганди і агітації, політики одностороннього інформування (до речі, не тільки не ігноруючи останній, а навпаки, підносячи його в окремих випадках до рівня спеціальних операцій), а й дедалі більше набуває якостей політики масової комунікації, обміну думками, активізації творчих здібностей людини заради суспільного блага.

Нині, на новому витку розвитку цивілізації, нового звучання набуває думка Арістотеля, яку він висловив у перших рядках своєї книги «Політика»: «...Будь-яка держава є свого роду спілкування, будь-яке ж спілкування організовується заради якого-небудь блага...»¹⁹.

Концепт інформаційної політики в сучасному світі був би не повним, якби ми обмежилися лише позитивними аспектами інформатизації суспільства, яка в науковому і технічному аспектах являє собою позитив, водночас у соціальному плані новий етап цивілізаційного розвитку людства, заснований на новітніх інформаційних технологіях, поряд з очевидною користю для особи, суспільства, держави, породжує і ряд нових не-

безпеки, які можуть набути не тільки негативних, а й загрозливих форм у разі проведення державою і державами незбалансованої і нерегульованої політики інформатизації.

Однією з основних проблем, без розв'язання якої навряд чи можна вести мову про побудову інформаційного суспільства, є складніша соціально-політична проблема забезпечення вільного доступу до світового інформаційного фонду, на думку М. М. Моїсеєва, ця проблема «навіть чи може бути розв'язана в рамках сучасних «привласнюючих» цивілізацій»²⁰. Вирішення суперечностей між об'єктивно суспільним характером знань і очевидною користю від одноосібного володіння інформацією та знаннями вимагає зміни цивілізаційних парадигм.

Негативні наслідки інформатизації, які можуть надати цьому процесу антигуманного характеру, поділяють на прямі та побічні (непрямі).

З позицій сучасної науки до можливих прямих негативних наслідків інформатизації відносять:

- загальний повний контроль над особистістю;
- «інформаційний тоталітаризм»;
- «інформаційну експансію» і «інформаційний імперіалізм»;
- «інформаційну цензуру».

Непрямими негативними наслідками інформатизації можна назвати:

- структурні зміни в суспільстві;
- підвищення вимог до інтелектуального і освітнього рівня членів суспільства;
- деперсоналізація знань;
- перерозподіл інтелектуальних функцій між людиною і «машиною»;
- домінування алгебраїчного, логічного мислення над геометричним, образним;
- прискорення соціальних процесів за рахунок підвищення ефективності зворотних зв'язків.

Не вдаючись до розкриття зазначених негативних наслідків інформатизації, зазначимо лише таке: інформатизація як така не розв'язує соціальних проблем і не визначає соціальної спрямованості перетворень, вона лише створює умови для прискорення процесів обміну інформацією, зміцнює інформаційні зв'язки в суспільстві, у тому числі й зворотні.

З теорії управління відомо, що наявність у системі негативних зворотних зв'язків стабілізує систему в цілому, якщо у контексті нашої теми — робить суспільство більш стабільним.

Наявність у системі позитивних зворотних зв'язків призводить (за збільшення коефіцієнта зв'язку) до її нестабільності, «розхитування», «генерації». Якщо йдеться про соціальну систему, то позитивні зворотні зв'язки при їх посиленні в процесі інформатизації можуть зробити її нестабільною. Тому будь-яка соціальна нерівність у суспільстві, що здійснює процес інформатизації, за наявності позитивного зворотного зв'язку по джерелу виникнення цієї нерівності буде посилюватися, переводячи суспільство у нестабільний стан. Так, у суспільстві, «в якому багаті багатіють, а бідні стають біднішими, за інформатизації відбудеться різке розшарування суспільства на дуже багатих і дуже бідних. Антагонізм між ними посилиться, що в підсумку призведе до соціального вибуху»²¹.

Інформатизація тоталітарного суспільства за наявності відповідних позитивних зворотних зв'язків призведе до крайніх форм тоталітаризму — до інформаційної тоталітарної держави, яка, за певних умов, може бути досить стабільною. Навіть інформатизація демократичної держави за наявності певних деяких тенденцій до тоталітаризму, за певних умов, наслідком може мати те саме — інформаційний тоталітаризм.

Розглядаючи проблему влади, її організаційну та соціокультурну роль у долях людей, народів, держав і людства в цілому, російський академік В. Ф. Халіпов (серед понять, які характеризують конкретні види і прояви влади, тільки «кратій» він визначає майже 60) пише: «Інформократія (від лат. information — ознайомлення, роз'яснення) — влада інформації, яка фактично повною мірою починається з розвитком інформатики в інформаційному суспільстві, спонукає до застереження про можливість інформаційної диктатури у XXI столітті»²².

Майже 30 років тому відомий американський фахівець з систем обробки даних Р. Тироф звертав увагу на важливість захисту інформації про особу в процесі впровадження інформаційних технологій: «Суспільству доведеться зіткнутися не тільки з такими проблемами, як адаптація до електронних грошей і безперервного зростання технологічного безробіття, яке посилиться у результаті впровадження обчислювальних машин, але перед

ним постане і проблема втручання в приватне життя громадян. І Оскільки центральні банки даних урядових організацій, кредитні бюро, ощадні та судні банки, а також інші подібні установи будуть централізованими, минуле індивіда може вельми відбитися на його майбутньому. ... Втручання в приватне життя громадян і порушення свободи особи може стати причиною того що велика кількість людей відвернеться від нашої капіталістичної системи»²³.

Чітке уявлення про концепт інформаційної політики, усвідомлення гостроти проблем, що існують в інформаційній сфері суперечливі процеси інформатизації і глобалізації вимагаюче системного підходу до аналізу системи державного управління інформаційною сферою загалом і її конкретної складової — системи державного управління національними інформаційними ресурсами — зокрема²⁴.

1.2. ВАЖЕЛІ ПРОЦЕСУ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО НАУКОВО-ТЕХНОЛОГІЧНОГО РОЗВИТКУ В УКРАЇНІ

19 лютого 2003 року набув чинності Закон України «Про пріоритетні напрями інноваційної діяльності в Україні», який визначено правові, економічні та організаційні засади формування та реалізації пріоритетних напрямів інноваційної діяльності в Україні. Статтею 7 цього закону на період 2003 — 2012 років визначені стратегічні пріоритетні напрями інноваційної діяльності:

- модернізація електростанцій; нові та відновлювані джерела енергії; новітні ресурсозберігаючі технології;
- машинобудування та приладобудування як основа високої технологічного оновлення всіх галузей виробництва; розвитку високоякісної металургії;
- нанотехнології, мікроелектроніка, інформаційні технології телекомунікації;
- удосконалення хімічних технологій, нові матеріали, розвиток біотехнологій;
- високотехнологічний розвиток сільського господарства переробної промисловості;
- транспортні системи: будівництво і реконструкція;

— охорона і оздоровлення людини та навколишнього середовища;

— розвиток інноваційної культури суспільства.

Правовою основою формування та реалізації пріоритетних напрямів інноваційної діяльності є Конституція України, закони України «Про наукову і науково-технічну діяльність», «Про державне прогнозування та розроблення програм економічного і соціального розвитку України», «Про інноваційну діяльність», «Про наукову і науково-технічну експертизу», «Про пріоритетні напрями розвитку науки і техніки», «Про спеціальний режим інвестиційної і інноваційної діяльності технологічних парків», інші закони України, Концепція науково-технологічного та інноваційного розвитку України²⁵.

Основою для підвищення ефективності науки має бути правильний вибір тематики наукових розробок. Неефективність витрат на науково-дослідні й дослідно-конструкторські роботи (НДДКР) зумовлюється головним чином помилковістю цільової орієнтації.

Труднощі вибору пріоритетів у наукових дослідженнях зазвичай бувають двох видів — свого роду «ідеологічні» й «технічні». Під першими слід розуміти те, що оцінка конкуруючих альтернатив розвитку досліджень завжди сягає своїми коренями в ієрархію фундаментальних ціннісних орієнтацій тієї чи іншої суспільної системи. Цінність дослідження може мати і загальнолюдський характер, водночас окремі наукові досягнення однієї країни іноді не представляють практичного інтересу для іншої.

Подолання труднощів ідеологічного характеру у визначенні пріоритетів, як вважає В. І. Терещенко²⁶, зв'язано з подальшим розвитком суспільних наук і проведенням постійних соціологічних обстежень з метою виявлення фундаментальних цінностей даного суспільства.

Цілком закономірно прагнути до того, щоб результати кожного проведеного наукового дослідження були не нижчими світового рівня. Однак з цього ще не випливає, що віддавати пріоритет розв'язанню якої-небудь проблеми потрібно лише на тій підставі, що вона розв'язана десь краще, ніж у нас. Визначення пріоритетів є важким завданням ще й тому, що ідеологічні цінності не піддаються точному кількісному аналізу.

В.І. Терещенко, який був директором так званого дослідницького «Кооперативного проекту» в Нью-Йорку у 1937 — 1946 роках, наводить такий приклад. Коли в 1960 році один із комітетів з наукових досліджень Конгресу США зіткнувся з проблемою визначення пріоритетів і звернувся за порадою до Американської академії наук, відповідь останньої свідчила, що будь-яке питання взаємозв'язку технології і людських цінностей легко переходить у розряд безлічі питань, пов'язаних і найгострішими проблемами людської цивілізації.

Питання про пріоритети досліджень потребує уточнення й у питанні про те, в чий інтерес робиться вибір. Він цілком логічний у світі ринкових відносин з усіма притаманними їм антагонізмами класових і групових інтересів.

Свого роду «ідеологічними» труднощами при визначенні пріоритетів є і питання критеріїв, які застосовуються при їхній оцінці, причому будь-яке дослідження має оцінюватися не зі проміжними, а за кінцевими результатами.

При встановленні пріоритетів у дослідженнях виникають численні «технічні» труднощі. Насамперед різноманітність досліджень, як і невизначеність їхніх результатів, призводить до відсутності загального знаменника для порівняння окремих розробок, що викликає необхідність багатокритеріальної оцінки варіантів рішень. Складність порівняння підсилюється й тим, що значні проблеми в наш час мають, як правило, міжгалузевий характер. При фундаментальних дослідженнях потрібно враховувати не тільки їхню власну значущість, а й питому вагу прикладних результатів, які вони можуть мати.

Визначаючи пріоритетні напрями наукових досліджень, необхідно забезпечити пропорційність і збалансованість розвитку цієї національної економіки.

Іноді результат досліджень, що здається в даний момент не важливим, може через якийсь час стати життєво необхідним, тобто критерії пріоритетності змінюються упродовж тривалого, так і коротких проміжків часу: проблема якості надійності вивела на перший план критерій оцінки очікуваних результатів досліджень і з цього погляду.

Одним із критеріїв пріоритетності має слугувати проективна тривалість дослідження. Ця проблема ускладнюється тим, що плановані терміни досліджень, як правило, не витримують

ся, причому не тільки зблизь зупинили їх продовження. Так, розвиток мікроелектронних схем відбувався у світі значно швидше, ніж передбачалося, тому розробки устаткування з застосуванням мікросхем досягли в 1960 — 65 роках рівня, що намічався на 1970 рік.

У зв'язку з цим зауважимо, що встановлена пріоритетність нерідко потребує коригування. Тоді як 25-літні демографічні цикли (період відтворення одного покоління) залишаються величиною постійною, технологія й асортимент продуктів у ряді галузей промисловості змінюється настільки швидко, що планування на п'ять років перетворюється на довгострокове.

Терміни перегляду пріоритетів залежать від наявної прогнозованої інформації. Ця обставина тісно пов'язує визначення пріоритетів із прогнозуванням і плануванням. Важливо зазначити, що, зокрема у США, під «планом» розуміють схему організаційної діяльності, тоді як «планування» інтерпретується як безперервний процес вивчення нових шляхів і методів оптимізації цієї діяльності за рахунок нових можливостей.

У своєму сучасному вигляді прогнозування, як відомо, стало розвиватися у фірмах США наприкінці 1950-х — на початку 60-х років — з появою ЕОМ. Прогноз є джерелом як плану, так і вибору тематики досліджень, а пріоритетність у останніх значною мірою визначається характером прогнозів, оскільки директивність у виборі тематики наукових досліджень і встановлений пріоритет залишаються недійсними, якщо немає умов, що дають змогу виконати поставлене завдання. Звідси — прогнозування є науково-аналітичною передумовою планування.

Якщо під науково-технічним прогнозуванням розуміти систему тільки ймовірнісних оцінок можливостей шляхів розвитку науки і техніки, їхніх очікуваних результатів, а також визначення необхідних для цього ресурсів, то при оцінці пріоритетів у дослідженнях уже йдеться про детермінування поставлених завдань. Прогнозування потрібно розглядати як процес пізнання, а планування — як процес впливу на об'єкт, виходячи з наявних можливостей. Прогноз має орієнтувати на пошук розв'язання проблем і зосереджувати увагу на пріоритетних завданнях.

За такого розуміння єдності процесу прогнозування, планування і різних аспектів концепції пріоритетності можна підхо-

дити до розгляду взаємозв'язку між установленням пріоритети у наукових дослідженнях і загальною системою організації управління ними²⁷. Ще 30 років тому стосовно програмного управління наукою В. М. Глушков, Г. М. Добров і В. І. Терещенко висловили думку про те, що системний підхід до розв'язання комплексу центральних проблем управління найбільш притаманний поширеному останніми роками новому і перспективному; підходу до керівництва наукою, так званому програмному управлінню.

У контексті сказаного, на думку автора, позитивним є факт визнання керівництвом де рукави, зокрема Прем'єр-міністром України В.Ф. Януковичем на науково-практичній конференції «Утвердження інноваційної моделі розвитку економіки України» того, що подальший інтенсивний економічний розвиток уже не може продовжуватися на існуючій виробничій базі. За висновками експертів, через недовикористання сучасних досягнень науки і техніки Україна втрачає мільярди доларів США.

Упродовж останніх трьох років фінансування інноваційної діяльності не перевищувало одного відсотка ВВП, а частка бюджетних асигнувань у фінансуванні інновацій зменшилася до 0,3%. Від недостатнього захисту інтелектуальної власності щороку наша країна втрачає близько 1 млрд. дол. США.

Для переходу до інноваційної моделі розвитку Кабінет Міністрів України передбачає реалізацію ряду таких заходів: І

- перебудувати державне фінансування наукової сфери за принципом програмно-цільового планування і безпосередньої пов'язаності з можливостями бюджету;

- ретельно переглянути всі державні інвестиційні та науково-технічні програми, зосередити фінансування виключно на найбільш затребуваних реальною економікою розробках;

- забезпечити постійний моніторинг інноваційних процесів та забезпечити оперативне реагування держави на особливості їх розвитку;

- створити систему фінансово-кредитного забезпечення інноваційної діяльності;

- сприяти забезпеченню кредитними ресурсами комерційних банків, які надають довгострокові кредити для реалізації інноваційних проектів;

- кардинально поліпшити діяльність Української держав-

ної інноваційної компанії, створити Банк розвитку та реконструкції;

- у співпраці з Верховною Радою України законодавчо забезпечити створення інноваційних небанківських фінансових інституцій, вдосконалити систему трансферу технологій та оцінки об'єктів інтелектуальної власності;

- приділяти увагу розвитку інфраструктури інноваційної діяльності;

- удосконалювати механізми діяльності технологічних парків, зокрема, підвищити вимоги до відбору інноваційних проектів, встановити жорсткий контроль за діяльністю технопарків, на базі яких відпрацювати модель прискореного функціонування в інноваційному циклі «наука — технологія — виробництво — сфера споживання»;

- започаткувати створення мережі нових інноваційних структур: венчурних фондів, технологічних бізнес-інкубаторів, промислово-фінансових груп, інжинірингових центрів;

- поставити завдання щодо створення інформаційних баз даних для забезпечення повною науково-технічною інформацією інвесторів, підприємств та органів влади;

- розширити міжнародне співробітництво в інноваційній та науково-технічній сфері²⁸.

Як позитивний факт можна розцінювати висловлену урядом впевненість у тому, що інновації для України — це безальтернативний шлях до новітніх технологій, світових ринків, модернізації економіки, забезпечення умов сталого людського розвитку. На жаль, втрачено надто багато часу, матеріальних і людських ресурсів, щоб дійти думки сформулювати відповідні концептуальні підходи.

Об'єктом управління наукою є науковий процес, і якщо уряд має наміри відпрацювати модель прискореного функціонування в інноваційному циклі «наука — технологія — виробництво — сфера споживання», то слід нагадати, що ще 30 років тому, за часів СРСР, наука перетворилася на складну систему, і вже тоді перед нею на весь зріст постало завдання переходу від екстенсивних до інтенсивних форм розвитку, управління наукою вступило в період системного впливу на всю сукупність зв'язків і відносин, що виникають у процесі науково-дослідної роботи. Ці відносини можуть мати дуже різноманітний конкрет-

ний характер. А зв'язки, в яких вони втілюються, можна розподілити на такі основні групи: *інформаційні* (включають вплив конкретних наукових ідей); *організаційні* (включають службово-правові відносини в колективі); *економічні* (включають відповідні стимули і форми відповідальності); *соціально-психологічні* (включають морально-етичні норми відносин у науці). Саме ці зв'язки об'єднують розрізнені елементи й акти наукової діяльності в єдину систему. Управління науковим процесом може бути успішним, коли вдається забезпечити ефективне функціонування всього комплексу названих зв'язків. Чим півнішій комплекс керованих зв'язків і чим дієвіше вони функціонують, тим життєздатнішою є наукова система і вищим є рівень її роботи. З цього випливає такий *принцип науково обґрунтованого управління наукою, як забезпечення єдності інформаційних, організаційних, економічних і соціально-психологічних зв'язків у процесі наукової діяльності*TM.

Встановлено, що в рамках *інформаційних* моделей циклу «наука — техніка — виробництво» управління прагне забезпечити випереджаюче зростання накопичення ідей і можливості техніки стосовно виробництва, а науки — стосовно техніки. Водночас у рамках *економічних* моделей того ж циклу «наука — техніка — виробництво» звичайним і раціональним є прагнення забезпечити випереджаюче зростання економічних показників порівняно з розмірами затрат. У рамках *організаційних* моделей циклу «наука — техніка — виробництво» справедливою і очевидно, однаково високого рівня і темпів удосконалення організаційних параметрів та характеристик керованої системи³⁰. Отже, комплексний системний підхід до завдань управління, теоретична обґрунтованість рішень і врахування реальної специфіки керованих систем — ще один важливий принцип сучасного управління наукою.

Яким би не був конкретний зміст прийнятих рішень, потрібні мати три основних компоненти, що відповідно визначають абі коригують цілі, шляхи їх досягнення і розподіл ресурсів. Якім проаналізувати всі невиконані рішення (або виконані, але неповною мірою), то можна встановити одну загальну причину для більшості з них: у цих рішеннях, як правило, або зовсім були відсутні один — два із зазначених основних компонентів! або було порушено узгодженість їх конкретного змісту. Звідс*

впливає *один із найважливіших загальних принципів прийняття раціональних управлінських рішень: системна погодженість і обґрунтованість вибору цілей, визначення програм роботи і розподілу ресурсів (принцип ЦПР)*⁹.

Враховуючи те, що сучасні бізнес-процеси не просто характеризуються швидкоплинністю, а ряд з них уже тепер здійснюється виключно у «віртуальному середовищі», тобто з використанням інформаційних ресурсів і технологій, за допомогою того ж Інтернету, використання математичних моделей, реалізованих у програмному забезпеченні інформаційних систем, що дає змогу істотно підвищити обґрунтованість прийняття рішень.

При прийнятті рішень, а будь-яка діяльність є ланцюгом прийняття рішень, необхідно відповісти на кілька запитань, мінімальний перелік яких становить: «Хто?», «Що?», «Де?», «Коли?», «Як?», «Скільки (наскільки)?» Інколи ми чуємо, в тому числі з високих трибун: «Керуймося здоровим глуздом!». Наскільки така постановка питання правомірна у вирішенні архіскладних питань державного рівня, в тому числі щодо науки, освіти, охорони здоров'я, пенсійної реформи, ядерної енергетики, військово-промислового комплексу, оборони тощо? Інтелектуальні й фізичні можливості людини дуже прискіпливо вивчалися наукою, особливо на етапі підготовки до польотів у космос. Людина як біологічний вид має досить конкретні і часто обмежені з урахуванням складності існуючих проблем можливості як фізичні, так і інтелектуальні, що безпосередньо впливає на її здатність до прийняття оптимальних рішень. Не зайвим буде нагадати, що історично управління і безпосереднє виконання робіт тривалий час здійснювалося одними і тими самими людьми, тобто система управління і об'єкт управління були єдиним цілим. З ускладненням завдань управління виник *перший інформаційний бар'єр*, який визначається пропускнуою спроможністю окремої людини як системи управління — 2-4 біт/с. Перший інформаційний бар'єр людство пододало шляхом відокремлення функцій системи управління від функцій об'єкта управління і переходу до ієрархічного принципу управління. У 70 — 80-х роках минулого століття, за визначенням академіка В. М. Глушкова, суспільство постало перед *другим інформаційним бар'єром* у сфері управління, подолання якого здійснюється нині шляхом автоматизації всіх інформаційних процесів, телекому-

нікації та мережевої технології. Тобто, якщо перший інформаційний бар'єр було подолано організаційними засобами, другий можна буде подолати лише високотехнологічним методом, який потребує не тільки знань основ управління, а й порційного розвитку всіх компонентів інформаційного простору. У такому разі об'єктом автоматизації стають функції завдання і процеси, які здійснюються в системах управління. А завдання удосконалення сприймається як завдання оптимального синтезу систем з управлінням: при заданих параметрах і множині зовнішніх впливів збудувати систему, яка забезпечувала б задану поведінку системи і відповідала критеріям якості управління. У силу ризикованості і великої вартості часто неможливо застосувати натурні експерименти, тому за основний метод досліджень складних систем використовують метод машинного експерименту — універсальний метод пізнання, заснований на використанні системних імітаційних моделей. Нагадаємо, що теорія прийняття рішень у своєму розвитку пройшла три стадії.

На першій стадії розвивався *дескриптивний підхід* до прийняття рішень: внаслідок проведених досліджень ученими було встановлено, що більшість людей діють інтуїтивно, проявляючи при цьому непослідовність і суперечливість у своїх судженнях. Саме на цій стадії було отримано досить чітку відповідь на запитання, що може і чого не може людина, яка вирішує за дання вибору.

На другій стадії дослідниками було запропоновано *нормативний підхід* до прийняття рішень, однак і він не знайшов практичного застосування, оскільки ідеалізовані теорії були розраховані на надраціональну людину з могутнім інтелектом.

Найрезультативнішою була третя стадія, на якій набув розвитку *прескриптивний підхід* до прийняття рішень. Він передбачав, як має діяти людина з нормальним інтелектом, яка хоча й напружено і систематизовано осмислити всі аспекти свого завдання. Цей підхід не гарантує віднайдення оптимального рішення в будь-якій ситуації, але забезпечує вибір такого рішення, яке не було б обтяжене суперечностями та непослідовностями. Водночас зазначений підхід висуває до людини серйозні вимоги щодо засвоєння нею методів і прийомів теорії прийняття рішень, а також потребує проведення численних розрахунків, тому для

підтримки процесу прийняття рішень на всіх його фазах на базі сучасних ПЕОМ розроблені і застосовуються програмні інформаційні системи³². При цьому не буде зайвим нагадати, що для одержання достовірного результату вхідна інформація такої системи має адекватно відображати реальний стан досліджуваного процесу або явища.

Математична модель досліджуваного процесу (явища), його алгоритми і практична програмна реалізація є ядром акумульованого інтелекту в системах автоматизації організаційного управління. Саме тому інформація з основ побудови систем автоматизації організаційного управління недоступна для широкого загалу й охороняється як комерційний секрет фірм — системних інтеграторів³³.

Розв'язання порушеного у даній монографії кола проблем було б реальним кроком на шляху вдосконалення системи державного управління системи національних інформаційних ресурсів з наукового потенціалу України з метою їх високоефективного використання, кроком до інформаційного суспільства. У цій справі фахівці знають, куди йти і що робити, але кожний народ, кожна країна має пройти цей шлях самостійно, мобілізуючи насамперед власні інтелектуальні, науково-технічні та технологічні можливості; і те, як ми зможемо вирішити ці завдання, багато в чому визначатиме обличчя і статус України серед інших країн світу в другій половині XXI століття.

Науково-технічний прогрес, визнаний у всьому світі найважливішим чинником економічного розвитку, останніми роками дедалі частіше ототожнюється з інноваційними процесами. Реаліями процесу глобалізації став вплив на його перебіг транснаціональних фінансово-промислових угруповань, які технологічно, географічно і політично диверсифікують свої рішення щодо широкомасштабних науково-технічних проектів.

Останнім часом зроблено багато заяв і розроблено чимало концепцій економічного розвитку України на засадах наукоємних технологій. Підставою для такого твердження є велика культурна традиція і значні можливості українських наукових шкіл і науково-виробничої бази.

Вступаючи у XXI століття, Україна наполегливо шукає своє місце в світовому економічному просторі в умовах жорсткої конкуренції і політичної кон'юнктури, коли людство усвідомило,

що лише високі та екологічно безпечні технології, інформатив-
зація й інтелектуалізація управління на засадах високої куль-
тури і моральності політичної й технічної еліти та населення
визначають імідж і значення держав у світі та на світовому ринку
товарів та послуг.

Це підтверджує нинішня ситуація, яка складається довкола
у світі, ініціативи США щодо створення нової системи протираї-
кетної оборони. Вона яскраво свідчить про підготовленість світо-
вого наукового співтовариства до нового ривка у напрямі ре-
лізації своїх ідей у сфері високотехнологічних виробництв.
Полеміка політиків не надовго затримає вихід визрілих у нау-
ково-технологічному комплексі США ідей, бізнесові інтереси
провідних промислових і банківських структур схилять їх де-
прийняття рішення про використання гігантських бюджетних
коштів своєї країни для технічного й технологічного переозб-
роєння США заради завоювання світових ринків високотехно-
логічної продукції.

Зрозуміло, що в цьому процесі буде задіяне все світове
наукове співтовариство, оскільки протягом останнього десяти-
ліття зусиллями США створено необхідну інфраструктуру і тех-
нології електронних комунікацій, проведена «геоінвентаризація»
наукових шкіл, у тому числі на пострадянському просторі;
відпрацьовані методики і схеми залучення необхідних фахівців —
носіїв ідей і знань — до розробки нової техніки й технологій.
Цей процес називають «вимиванням», «відтоком мізків», проте
це нормальне явище, зумовлене інтелектуалізацією праці на-
селення США, їх системною і послідовною політикою в цьому
напрямі упродовж усього XX століття.

Відомо, що меншою мірою цього змогли досягти упродовж
останніх двадцяти років усі індустріально розвинуті країни
шляхом розвитку менеджменту і соціальної організації своєї
науково-технічної еліти.

Історики України ще мають проаналізувати, скільки відки-
нутих українською науковою аристократією вчених і фахівців
нашої країни реалізували себе на Заході, але сьогодні важли-
во визнати й усвідомити, що осмислення і науково обґрунтова-
не прогнозування використання інтелекту українського народу
стало предметом стратегічних досліджень провідних корпорацій
світу.

Інженерно-технічна еліта України усвідомлює, що харак-
терною ознакою світового ринку буде велика кількість товарів,
вироблених на основі високих, подвійних технологій, і що інте-
реси США і Західної Європи будуть досить суперечливими. Тому
Україні належить обстоювати свої національні інтереси та упе-
реджувати такий однозначний розвиток подій. Відкидаючи на-
в'язувану нам роль сировинного придатку та поважаючи свій
соціальний статус, найбільш далекоглядні керівники промисло-
вих підприємств України об'єднуються навколо міжнародних
аерокосмічних проектів, проектів у галузі літако- та суднобу-
дування, розширюють свій вплив на ринках озброєнь. Зокрема,
на виставці 2001 року в Абу-Дабі українські промисловці про-
демонстрували свої ресурси, наміри і можливості у створенні
високоточної зброї, надавши Україні статус третьої у світі краї-
ни, яка має необхідний науково-технічний і виробничий потен-
ціал для цього.

Досвід таких досягнень засвідчує, що Україні конче необхід-
но зосереджено проаналізувати накопичені інформаційні ресурси
в галузі високих і наукоємних технологій, визначити на дер-
жавному рівні не тільки наукові, а й науково-технічні пріори-
тети, спроможні надати державі валютні коридори до світово-
го ринку товарів і послуг, консолідувати творчі сили й ресурси
суспільства. Треба створювати не зразки, а системи озброєнь,
як це робиться протягом останніх сорока років у США і робило-
ся в колишньому СРСР, а тепер — у Росії. Варто переосмисли-
ти й удосконалити систему управління науково-технічним і обо-
ронно-промисловим комплексом країни.

А найголовніше, потрібно визначити стратегічні цілі держа-
ви, в тому числі у науково-технічній сфері й оборонно-промис-
ловому комплексі, сконцентрувати ресурси для їх досягнення,
реорганізувати систему управління ними так, як підказує влас-
ний досвід і розуміння змін у внутрішньому і зовнішньому сере-
довищі. Національна наука і національна промисловість здатні
ефективно працювати лише за наявності соціально значущої
та чітко поставленої державою мети. Якщо не визначити тако-
го завдання для науково-технічної еліти України і надалі не
використовувати інтелектуальний потенціал нації для розв'я-
зання суспільно значущих проблем, є всі підстави стверджува-
ти, що він стане працювати на інших. Ми самі інколи недооці-

нюємо рівень вітчизняних фахівців. У зв'язку з цим доречно навести висловлювання професора Массачусетського технологій*ного інституту Лестера Туроу, який набув всесвітнього визнання як провідний фахівець у галузі економіки: «Колишнім Радянський Союз був суспільством, високо оснащеним наукою здатним робити найдосконаліше озброєння, суспільством, яке запустило удвічі більше космічних ракет, ніж Сполучені Штати. Усі ці інженери та вчені не зникли. Вже є американські компанії, котрі організували інженерні групи у Санкт-Петербурзі та Москві, якими можна керувати з Каліфорнії або Массачусетса за допомогою електронного зв'язку»³⁴.

Справді, володіння Україною значним інтелектуальним інформаційним ресурсом завжди обумовлювало перспективу прогресу її розвитку і сьогодні надає можливість зайняти гідне місце у світовому співтоваристві, однак формування сучасних концепцій інформаційних моделей, які однозначно та досить повно описують систему державного управління інформаційними ресурсами, – складний, а часом і суперечливий процес. Це пояснюється, перше, тим, що в умовах глобалізації інформаційні ресурси стають головним і найбільш цінним стратегічним ресурсом держави, а їх власниками все більше – їхні творці, тобто окремі особи, по-друге, тим, що Україна не досягла не тільки рівня суспільно-економічних відносин постіндустріальних країн, таких як США, провідні країни Європи та Японія, а й відповідного ставлення до інформаційних послуг, інформації загалом. У розвинутих суспільствах знання, вміння видобути з інформації користь, перетворити, застосувати її є потребою підприємництва. До того ж в Україні до цього часу не сформульована економічна мета – в нас все підпорядковано вирішенню політичних питань, а нам конче потрібно не декларувати, а сформувати саме європейську концепцію економічного розвитку. Країни Європи постійно вивозять більше, ніж ввозять, у них позитивне сальдо торгового балансу, невеликий державний борг, висока допомога по безробіттю, що майже не відрізняється від зарплати.

Орієнтуючи вектор розвитку України до Європи, слід відверто робити наголос і на тому, що в нас не тільки більшість людей неспроможна керувати своїм майбутнім у соціальній ієрархії, а й сама еліта не в змозі цього робити. На Заході ж вона є дурею

динамічною. Попит, зміна обставин зумовлюють постійну ротацию керівників усіх рівнів. В Україні ж одні й ті самі особи протягом багатьох років керують і контролюють усі соціально-економічні процеси. Як наслідок, ми не можемо задіяти в обіг ініціативу і творчий потенціал власного народу, що спричиняє основну проблему сучасної України з погляду відповідності європейським стандартам – це її економічна слабкість, на яку накладається інституціональна слабкість влади.

Пріоритетною є роль, яку відіграє інститут приватної власності в сучасних західних країнах, сформованої у глибині століть у процесі переходу західноєвропейських соціумів від варварства до стану цивілізованості і зумовленої особливостями функціонування економік. Розвиваючись за рахунок удосконалення засобів виробництва, а не оптимізації управління, їхня економіка споконвічно формувалася як автономна і самодостатня система, ефективність функціонування якої залежала не стільки від діяльності владних структур, скільки від ефективності функціонування інституту власності, що поступово стає системоутворюючим ядром соціально організованої структури. Генеральним суб'єктом соціальної дії і головним гарантом їхнього демократичного устрою – при порівняно нечисленному вищому (майнова еліта) і нижчому (найбідніша частина) прошарках – виступає середній клас як сукупність економічно самостійних соціальних суб'єктів.

У давньосхідних суспільствах (соціуми іригаційного землеробства і соціуми неполивного землеробства) ситуація складалася інакше. Включення владних структур безпосередньо у процес виробництва надало їм можливість посісти лідируюче становище у соціумі, позбавивши економіку самостійності й перетворивши її на свого роду функцію влади.

На жаль, Україна не переборола історичну спадщину, і тому ми досі маємо в економіці невеличку за чисельністю групу «людей влади» з переважною більшістю бідного населення, середніх прошарків практично немає.

Усі творчі процеси людського мислення являють собою здебільшого переробку великих обсягів інформації, людська комунікація на відміну від процесів передачі інформації в природі (наприклад, генетичних) включає складні функціональні системи, у тому числі діяльність і матеріальний субстрат мозкової

матерії. Вивчення цих явищ і суперечностей вчені тільки почи- нають, але визнано, що розвиток науки формує умови ефек- тивного відтворення «головної продуктивної сили» суспільства - \ інформаційних ресурсів. Саме наука і масштаби поширення на- укового світогляду впливають на динаміку, на механізм управ- ління соціально-економічними процесами, розкріпачують або щ навпаки, сковують розвиток продуктивних сил, визначаючи] зокрема, зміст економічної і політичної реформ в Україні, її деформацію і суперечливі результати. Протягом дванадцяти років незалежності декларується бажання стати європейською краї- ною з ринковою економікою, відтворюючи капіталізм початку минулого століття.

Будь-який рух до прогресу бере за основу інтереси власно] го народу. Західне постіндустріальне суспільство виникло так] де люди змогли перейти від суто матеріальних інтересів до значною мірою нематеріальних. Стати творцем, якщо ти жи- веш погано, неможливо, тому саме Європа і США, створивша в XX столітті своїм громадянам захищене соціально-економіч-] не середовище, утворили той єдиний полюс сили і впливу на світовий економічний (а отже, і політичний) порядок, із яком почалося XXI століття і в якому роль держави визначатиме™ ся кількістю населення і сировиною, здатністю нації створював ти принципово нові технології.

Відомо, що до початку ринкових перетворень у країні існи вав потенціал, який за багатьма характеристиками відповідай рівню найбільш розвинутих країн світу. Україна успадкувала від СРСР потужну інфраструктуру — у вигляді могутніх і чий ленних науково-технічних комплексів системи освіти і науки електричних мереж, транспортних магістралей тощо. Вітчизни на система відтворення інтелектуального потенціалу в 70 — 80-ї роках минулого століття, за визнанням учених світового рівня навіть у ситуації недосконалості економічного механізму, пере] вершувала рівні США і багатьох інших європейських державі Саме завдяки наявності цієї інфраструктури ми принципові відрізняємося від країн, що розвиваються. Крім того, систем* освіти, що існувала в країні, надавала певний мінімум знань (як час, засвідчив найкращий у світі) і уявлення про те, щ] отримані знання, не є остаточними, що є ще щось, що зали- шається за межами підручника. І тому авторитет ученого, тоб-

то людини, яка намагається сягнути за межі підручників, в Україні був досить високим.

Україна мала величезний науково-технологічний досвід у сфері розробки і впровадження технологій оборонно-промисло- вого комплексу, оскільки радянський період розвитку науки в Україні зумовлював створення, в умовах відносної ізоляції СРСР, могутнього самостійного наукового комплексу, здатного забез- печувати вирішення завдань оборони і безпеки. У спадщину від колишнього СРСР Україні залишився добре розвинутий військо- во-промисловий комплекс, до якого входило 1840 підприємств, де працювали 2,7 млн. осіб. Обслуговуючи потреби інтенсивної індустріалізації країни і форсованого розгортання воєнної про- мисловості, маючи високий рівень мілітаризації науки й вироб- ництва, Україна талановито інкорпорувала, розвиваючи запо- зичені зовні технологічні і культурні ідеї і погляди. Українські вчені досягли значних успіхів у галузі аерокосмічних, фізико- математичних, хімічних і біологічних наук. Водночас відбувався процес модифікації військових технологій у цивільні. Потреби «оборонки» проймали все українське суспільство, тому що існу- вали умови для проведення широкого фронту фундаменталь- них і прикладних досліджень, які охоплювали майже всі сфери знання.

Промислові підприємства, установи Академії наук і вищої школи України виконували і впроваджували результати фун- даментальних досліджень, створюючи основи новітніх техно- логій оптики, загального, надпровідникового, діелектричного і напівпровідникового матеріалознавства і пов'язаних з ними на- нотехнологій, кібернетики, засобів обчислювальної техніки, квантової електроніки, радіотехніки і автоматики для потреб військово-промислового комплексу, які сьогодні, власне, зу- мовляють перехід людства до нового технологічного укладу життя.

. Так, завдяки відновленню в повоєнному Києві функціону- вання заводу «Арсенал» як оптико-електронного підприємства українська наука і промисловість успішно розв'язали проблему виготовлення оптико-електронних приладів і систем світового рівня. Завод брав активну участь у перспективних досліджен- нях, спрямованих на підвищення обороноздатності країни³⁵. Саме завдяки цим розробкам радянська «Стрела-3» була прийнята на

озброєння на кілька років раніше, ніж її американський аналог - І «Стінгер». То був виклик світовому лідерству США.

Активне співробітництво вчених України з військово-промисловим комплексом СРСР у галузі напівпровідникової фотоелектроніки започаткувала конференція з фізики напівпровідників, проведена Інститутом фізики напівпровідників у Києві у 1957 році. З огляду на високу кваліфікацію українських учених і спеціалістів Чернівецького університету рішенням директивних органів СРСР у місті Чернівцях за короткий термін було побудовано завод «Кварц» для випуску фотоприймачів.

А з урахуванням потреби у фотоприймальних пристроях (ФПП) інфрачервоного діапазону 8 — 14 мкм на основі твердотелів розчинів телуриду кадмію і ртуті (КРТ), які сьогодні визнають рівень озброєнь, було споруджено завод чистих металів у місті Світловодську. Для розв'язання його енергетичних проблем використовувався каскад дніпровських ГЕС. На розробку вкрай складної технології отримання матеріалу КРТ у високорозвинутих країнах пішло понад 15 років, хоча розробники мали можливість купувати надчисті вихідні матеріали і прецизійні технологічне устаткування в усьому світі. У наших дослідників такої можливості не було. Однак спільними зусиллями проблема поступово розв'язувалася. І до 1983 року якість вітчизняного матеріалу була вже достатньою для створення багатоелементних ФПП, призначених для тепловізійних систем нічного бачення й автоматичного керування об'єктами техніки. А на початку 1990-х років цей матеріал за якістю перевершив відомі американські зразки, маючи нижчу вартість (загалом же КРТ удесятеро дешевший, ніж золото).

Маючи прямі бюджетні асигнування, оборонна промисловість владно створювала в Україні промислову й наукову інфраструктуру, іноді порушуючи та зміщуючи баланс соціальних інтересів. Свого часу, у 1984 — 1991 роках, мені довелося очолювати підрозділ Міністерства оборонної промисловості СРСР по координації науково-технічного співробітництва підприємств у галузі з установами Академії наук і вищої школи України і бібліотеки, який величезний внесок зробили українські фахівці в розвиток новітніх систем озброєнь, що сьогодні демонструють США і Росія, як напружено працювала Президія Академії наук УРСР, відстежуючи світові тенденції в організації впровадження у ви-

робництво наукових розробок, зокрема у співробітництві з ВПК СРСР³⁶.

Інноваційна політика є важливою складовою державної промислової політики. Вона визначає основні цілі інноваційної стратегії і механізми реалізації пріоритетних інноваційних програм і проектів. Головними і найгострішими проблемами інноваційної політики в даний час є підвищення ефективності використання наукових розробок, впровадження результатів фундаментальних, пошукових і прикладних досліджень у виробництво вітчизняної продукції, у тому числі військового призначення.

За роки радянської влади оборонно-промисловий комплекс країни набув значного розвитку. Це дало йому можливість вийти на передові позиції у світі по виробництву більшості видів озброєнь і військової техніки. У той час в країні діяли критерії не економічної рентабельності капіталовкладень, а досягнення переваги бойових показників вітчизняних зразків зброї над закордонними аналогами. Перед розроблювачами вітчизняної зброї стояло завдання не віднайдення фінансових ресурсів, а їх «освоєння», тому що кошти виділялися фактично в необмеженій кількості.

Як наслідок такої політики — у оборонно-промисловому комплексі був зосереджений величезний науковий потенціал і створено унікальний науково-технічний доробок.

У оборонно-промисловому комплексі СРСР функціонувало понад 5 тис. наукових організацій, де були задіяні 1,5 млн. висококваліфікованих спеціалістів. З усього обсягу фінансування НДДКР на частку оборонно-промислового комплексу припадало майже 80%.

Так, незважаючи на те, що за роки реформ у Росії не створено жодної нової системи зброї, аналіз технологічного напрямку розвитку науки і техніки у світі засвідчив, що в галузі військових технологій 69 російських розробок не поступаються кращим закордонним аналогам, а по 13 Росія займає лідируючі позиції у світі³⁷.

У 70 — 80-х роках ХХ століття у СРСР щорічно запускали в середньому 100 — 120 космічних літальних апаратів, значна частина яких мала оборонне призначення. Установи Академії наук України брали активну участь у розробці ракетно-космічних носіїв і апаратів, бортових приладів, у проведенні робіт,

спрямованих на розв'язання різних проблем космічного зв'язку, навігації тощо.

Штучні супутники Землі, які давно стали для земної цивілізації своєрідними електронними органами чуття, використовуються і сьогодні для потреб військових відомств. Так, до глобальних космічних систем розвідки, зокрема раннього попередження про запуск балістичних ракет, входять космічні телескопи, оснащені інфрачервоною апаратурою. Глибока розробка науково-технічних проблем у аерокосмічній сфері надає людству новітні технології, матеріали, біомедичні комплекси, мобільні технології зв'язку. Сьогодні без супутників погасли б екрани телевізорів і змовкли б мобільні телефони, втратили навігаційні кораблі, припинилося б надходження інформації, необхідної для метеорологічних і екологічних прогнозів.

Узагалі виготовленням ракетних носіїв ядерної зброї і аерокосмічної техніки українські учені та інженери довели широкому загалу свою виняткову корисність і надійність, що, зокрема, зумовило обрання в 1994 році Президентом України Л. Д. Кучми, який стояв біля витоків створення легендарної ракети «Зеніт» як помічник головного конструктора і керівник групи провідних конструкторів по ракетно-космічних комплексах³⁸.

Глобалізація економічних і політичних процесів і інформатизація суспільного життя робить наголос на інтернаціоналізації інформаційної діяльності у процесі переходу до формування так званого інформаційного суспільства, в якому одним із основних предметів праці більшої частини людей є інформація і знання, її знаряддям — інформаційні технології. Однак входження у глобальне інформаційне середовище не відмінює наявності національних інтересів і необхідності забезпечення їх безпеки, тому сьогодні для формування у світового співтовариства реальної уявлення про науково-технічний потенціал України, потрібно впровадити всебічно обґрунтовані (політичні, юридичні і соціальні) критерії цінності накопиченої змістовної інформації, оскільки їх на цей час в Україні немає.

На жаль, у багатьох з нас досі немає розуміння того, що за допомогою інтелектуальної власності можна одержати цілком реальні конкурентні переваги на ринку. Вона допомагає збільшити рівень капіталізації підприємства, оптимізувати оподаткування, підвищити інвестиційну привабливість і дохідність. Але поки

що лише окремі підприємства оцінюють об'єкти інтелектуальної власності, включаючи їх у вартість своїх активів.

Як відомо, всі попередні технологічні революції будувалися на безмежному використанні природних ресурсів, які сьогодні перебувають на межі вичерпання. Розуміння того є найважливішим показником зрілості суспільної свідомості і державної політики, якщо вона спрямована на вирішення завдань національного відродження і розвиток суспільства. Багато політичних діячів на конкретних прикладах трансграничних інформаційних операцій, у тому числі військового і терористичного характеру, довели, що нова загроза, або так звана неіснуюча війна, набула реальних обрисів.

Протистояння і конкуренція країн за володіння інформаційними ресурсами розвитку економіки тривають. Усвідомлюючи всю серйозність потенціальної загрози впливу на свої інформаційні ресурси, провідні країни на національному рівні почали реалізацію довгострокових програм, спрямованих на забезпечення інформаційної безпеки передусім критично важливих інфраструктур.

Здоровий консерватизм у сфері охорони науково-технічних знань виправданий. Щоб його зрозуміти, треба вивчити набутий у процесі протистояння наддержав досвід, коли у 1945 — 1985 роках у світі було створено унікальну систему у військово-стратегічній і науково-технологічній сферах. Такий підхід дасть змогу розглядати науково-технічний інформаційний ресурс, отриманий як специфічний ресурс розвитку конкурентоспроможної економіки і забезпечення національної безпеки.

Тому можна висловити припущення, що основні результати фундаментальних пошукових досліджень у найближчі 10 — 15 років матимуть воєнне спрямування. Крім того, зміни в навколишньому середовищі відбуваються дуже стрімко — реальність змінюється швидше свідомості. Людина навчається, а незабаром з'ясується, що її знання і навички вже застаріли, ті технології, що вона тільки-но засвоїла, більше нікому не потрібні. Саме звідси — нестабільність і незахищеність особистості перед лицем не контрольованих нею змін, тому доступ до результатів НДКР, отриманих фахівцями у процесі виконання фундаментальних та пошукових досліджень в інтересах забезпечення пріоритетності, обмежується. Тут варто зазначити, що

під результатами досліджень, до яких обмежується доступ необхідно розуміти не конкретний науковий результат (наприклад, «у результаті проведених досліджень було досягнуто...» і а технічні і технологічні умови, знання яких дає змогу іншим науковим колективам досягти цих результатів. Невиконання цього може призвести до повної ізоляції вченого від наукової світу, що в свою чергу не дасть йому змоги зіставляти отримані особисто ним результати з рівнем відповідних досягнень світі. І зусилля, затрачені на забезпечення відповідного рівня таємності, принесуть скоріше непоправну шкоду, ніж реальні користь. Межа, яка розділяє інформацію у галузі фундаментальних досліджень на відкриту та закрити, чітко не визначена, її визначають договірними відносинами між замовником та дослідження та виконавцем.

Не можна забувати, що економічні принципи створення озброєнь і вільний товарний ринок наукоємної продукції істотно відрізняються один від одного. Ринок озброєнь як і раніше тяжіє до планової економіки і формується залежно від необхідності забезпечення національної безпеки і наявності бюджетних коштів! Товарний ринок регулюється співвідношенням попиту і пропозиції і розвивається в умовах жорсткої конкурентної боротьби тому прибуток від використання подвійної технології на товарному ринку має бути переданий замовнику без будь-яких обумовлень. Більш того, замовник може передати право розпоряджатися об'єктом інтелектуальної власності будь-якій іншій фірмі.

Осмислення і узагальнення потребує аргументація прихильників успіху азійських країн щодо орієнтації України на вибір їхнього шляху розвитку. Сьогодні можна впевнено стверджувати, що успіх «азійських тигрів» було закладено американським і європейським бізнесом, потреби якого вони підтримують і які зникнуть тоді, коли це стане потрібно Заходу. Не варто ставити за приклад навіть Китай, економіка якого теж жорстко зорієнтована на потреби Заходу. Нам, європейцям за походженням, треба знайти таке розв'язання проблеми використання накопичених інформаційних ресурсів, щоб стати в колі країн, які здійснюють управління знаннями — ресурсом надзвичайної вартості. А поки що ми навіть не продемонстрували Заходу суспільства порядного, духовно високого і морально чистого.

Каркас у системі «наука — виробництво» в СРСР тримався на галузевих НДІ і КБ, академічних інститутах, університетах, окремих вузівських лабораторіях, науково-виробничих об'єднаннях. Здобуваючи нові знання під час фундаментальних досліджень, вчені й інженери створювали і засекречували їх майже в усіх галузях математики, фізики, хімії, механіки, біології, наук про Землю, впроваджували їх у новітні системи озброєнь, аерокосмічної техніки, приладобудування, суднобудування тощо. Тому сьогодні набуває актуальності проблема запровадження в обіг накопиченої такої інформації, відкритості інформації про наукові дослідження взагалі та використання їх результатів у міжнародних науково-технічних проектах.

Цілеспрямоване співробітництво науки з військово-промисловим комплексом у всьому світі розпочалося напередодні Другої світової війни як взаємодія близьких за напрямками досліджень лабораторій і підприємств оборонно-промислового комплексу, а з початком війни військовою тематикою опікувалися майже всі академічні інститути. Вона наочно довела і зумовила раціональність створення великих науково-виробничих комплексів, які в повоєнні роки об'єднали зусилля вчених академічних установ з промисловими підприємствами оборонних відомств усіх розвинутих країн.

Відсутність яскраво виражених меж між фундаментальною наукою та науковою технологією зумовили створення в Україні ще за радянських часів науково-технологічних комплексів у системі Академії наук, які, без перебільшення, відіграли винятково важливу роль у створенні механізмів ефективного впровадження досягнень науки у виробництво в умовах соціалістичної економіки і дістали гучну назву «патонівської школи». Сьогодні це стало світовою тенденцією. Відбувається переміщення науково-дослідницьких центрів до структур транснаціональних фірм, підпорядковане розв'язанню проблем комерціалізації «науку» («секретів виробництва») до рівня прикладних технологій, спрямоване на їх продаж і швидке впровадження у виробництво. Саме технології привертають сьогодні увагу світових виробників на проблематиці «науку», які мають бути захищені від несанкціонованого використання третіми особами, оскільки мають справжню або потенційну вартість саме тому, що невідомі третім особам, їх власник вживає належних за-

ходів щодо обмеження доступу, спонукаючи законодавців ефативніше вирішувати питання правового визначення понять «ноу-хау», «комерційна таємниця» і «державна таємниця».

Ноу-хау в контексті регулювання державою правових Відня син щодо трансферу технологій уявляється як конфіденційні інформація у вигляді документації про технології та їх об'єкти яка не є загальновідомою або легкодоступною на день укладення договору про трансфер технологій, зафіксована в установленому порядку на матеріальному носії інформації, є корисною та може надати переваги її одержувачу порівняно з іншими суб'єктами, а також є необхідною для забезпечення можливого застосування технологій, що передаються. Термін «ноу-хау» використовується для визначення наукових, технологічних і конструкторських секретів, які стосуються виробництва продукції та послуг, що надаються при здійсненні цього виробництва, знань управлінського, організаційного, комерційного, тобто, фінансового або іншого характеру, взаємопов'язаних розробкою і освоєнням технологій та їх об'єктів, виробництвом, реалізацією продукції, виготовленої з їх застосуванням, експлуатацією, обслуговуванням та ремонтом технологічного обладнання, яке входить до складу технологій, а також перелік порядку та послідовності виконання певних операцій технологічного процесу, навичок, виробничого досвіду, пропозицій удосконалення технологій, їх об'єктів і продукції.

На нашу думку, поняття «комерційна таємниця» істотно ширше, ніж «ноу-хау», оскільки комерційну таємницю можуть скласти, крім усього іншого, списки клієнтів, первинні бухгалтерські документи і багато інших відомостей. У свою чергу поняття «державна таємниця» ширше, ніж «комерційна таємниця». Державною таємницею можуть охоплюватися відомості, що не мають ринкової вартості, або ті, що ніколи не виходять в комерційні ринки. Водночас частина комерційної таємниці може належати до державної таємниці, що найбільш яскраво виявляється при торгівлі наукоємними озброєннями і військовою технікою.

За новими матеріалами й високими технологіями — добре організована система організації і захисту наукових досліджень. У контексті цієї праці під високими технологіями ми розуміємо технології, розроблені на основі новітніх наукових знань, що а

ють основними характеристиками відповідають рівню найкращих світових стандартів у певній галузі промислового або сільськогосподарського виробництва і спроможні забезпечити суб'єктам, яким передаються майнові права на них, передові позиції на світовому ринку наукоємної продукції. На ранніх стадіях наукового пошуку необхідність засекречування робіт визначається не лише сферою військового застосування, а й можливістю використовувати отримані результати для розв'язання агатових цивільних проблем, що привернуло увагу до захисту інформації, включаючи і відповідну інтелектуальну власність. Тому наприкінці 80-х років минулого століття у світі виникла принципово нова ситуація у конкурентній боротьбі високотехнологічних фірм і держав — на базі новітніх технічних розробок і виробництва малих серій спеціальної техніки (для перехоплення, запису, несанкціонованого копіювання і передавання користувачу інформації) виникло кваліфіковане промислове й інформаційне шпигунство (рис. 1), якому почали протистояти, крім режимно-секретних, підрозділи протидії іноземним технічним розвідкам.

Протидія технічним розвідкам стала завданням державної ваги однією зі складових у загальній системі заходів для збереження державної і службової таємниці, тому в СРСР для організації і координації робіт у цій галузі рішенням уряду в грудні 1983 року була створена Державна технічна комісія СРСР. У СРСР, США, Японії, провідних країнах Європи була створена добре розвинута система зовнішньої розвідки. У СРСР її координувала безпосередньо Державна комісія Ради Міністрів СРСР з військово-промислових питань, яка давала держзамовлення на створення новітньої військової і спеціальної техніки. Конфіденційна закордонна науково-технічна інформація допомагала підтримувати військово-промисловий паритет із США і країнами НАТО. У цілому така таємна діяльність має велике економічне значення для усіх високорозвинутих країн, даючи змогу за рахунок використання науково-технічних досягнень цих країн швидко й ефективно розв'язувати багато найважливіших окремих проблем, у тому числі на рівні окремих підприємств та акціонерних виробничих структур.

Високий науково-технічний рівень отриманої інформації, відкриває її застосування в оборонній промисловості забезпечу-

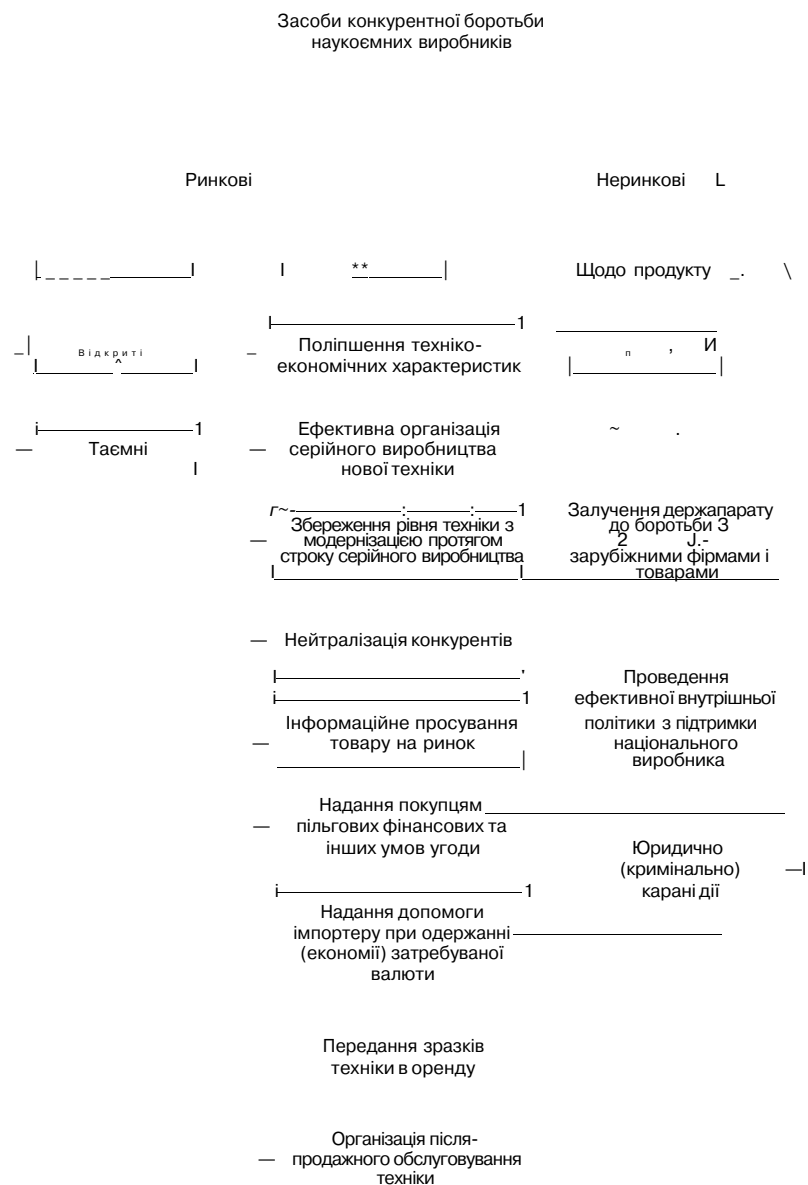


Рис. 1. Засоби конкурентної боротьби наукоємних товаровиробників

вало створення аналогів із підвищеними параметрами якості, новизни і технічного рівня тощо, виробів оборонної техніки і гнучких автоматизованих виробництв оборонної промисловості. Природно, витрати з одержання конфіденційної інформації, документів або зразків виробів нової техніки включали витрати на «хороше» життя розвідників, витрати на вербування спеціалістів, плату за інформацію і т.д., «перехресну» незалежну оцінку якості документів провідними вченими і спеціалістами.

Щоб сьогодні оцінити такі витрати, треба проаналізувати, наприклад, ситуацію, яка складається навколо системи стратегічної ПРО США.

За розрахунками вашингтонського Центру з контролю за озброєннями, реалізація всіх проектів стратегічної ПРО може обійтися США в 1,2 трлн. дол. до 2035 року. Розробка бойового хімічного лазера, що встановлюється на літаки «Боїнг—747», обійдеться американській казні в наступні тринадцять років ще в 11,2 млрд. дол. Найдорожчим проектом стане створення високоенергетичної лазерної зброї та її установка на низькоорбітальних супутниках. Це обійдеться в 423 млрд. дол.

За планом Пентагона, перша черга системи ПРО має розпочати своє функціонування в 2007 році. Проте вже сьогодні зрозуміло, що вкластися в ці терміни не вдасться, витрати можуть перевищити раніше заплановані більш як у десять разів. Це спонукало і США запропонувати в листопаді 2002 року об'єднати зусилля в створенні ПРО, в світлі чого старший віцепрезидент корпорації «Боїнг» (генпідрядник Пентагона по ПРО) і колишній посол США в Росії Томас Пікерінг провели попередні переговори з партнерами в Росії.

Інформація про представника корпорації «Боїнг» надана для уявлення того, що у високотехнологічних сферах бізнесу сьогодні працюють високоосвічені люди, головним чином, дипломати і розвідники, які для своєї нової професійної діяльності застосовують, по суті, секретні відомості, які стали їм відомі в силу їхньої попередньої секретної діяльності. Вони створюють у себе на батьківщині і в країнах колишнього перебування спеціалізовані наукоємні, технічно добре оснащені фірми, тобто ділова конкурентна і зовнішньоекономічна розвідка стають важливими інструментами конкурентної боротьби світових товаровиробників наукоємної продукції. Коментуючи наведену схему, можна по-

яснити поразку українських авіабудівників із проектом літака «Ан—70» у конкурентній боротьбі світових авіабудівельних компаній.

Специфіка господарського статусу вітчизняного науково-технічного доробку в сучасних умовах, коли в світі зріс попит на технології і матеріали, які замовлялися військовими, зумовила додаткову цінність його як інформаційного ресурсу держави, оскільки це принципово нові матеріали і технології, за якими — добре організована система наукових досліджень. Нові матеріали і технології змінюють один одного, вони з'являються безупинно, і за кожним новим матеріалом на підході наступний — із ще більш фантастичними властивостями і технологіями їх отримання в промисловому вимірі. Наявність такого науково-технічного потенціалу вимагає вироблення концептуальних підходів щодо його управління і використання в сучасних умовах, коли зміна форм власності на інформацію стосується особливу процесів трансферу технологій, зумовлює виникнення значних проблем технологічної безпеки держави, оскільки бурхливий розвиток інформаційних технологій зумовив розвиток методів здобування інформації економічною розвідкою.

У 1990-х роках в умовах фінансового неблагополуччя для більшості установ Академії наук і вищої школи України виявилося економічно вигідніше відмовитися від проведення секретних НДДКР. В окремих випадках це призвело до погіршення якості виконуваних наукових і виробничих функцій і, відповідно, до падіння конкурентоспроможності продукції.

Нагадаємо, що на початку 90-х років минулого століття пріоритетною вважали конверсію, у той період під тиском ультралібералів були сформульовані законодавчі обмеження на формування у високотехнологічному комплексі України промислово-фінансових груп. Ймовірно причини такого рішення, були суто політичними — побоювалися консолідації еліти оборонки.

Сьогодні Україна вкрай виснажена затяжною, глибокою економічною кризою, технологічною деградацією. На очах зникають наукові школи, оскільки талановита наукова молодь орієнтується на роботу в західних науково-промислових центрах. Жалюгідне існування багатьох вітчизняних НДІ і КБ — прямий наслідок некваліфікованого менеджменту за відсутності чіткої політики держави, яка є їх головним власником. Розрив науково

во-технологічних зв'язків, багаторазове зменшення витрат на науку, значне постаріння наукових, конструкторських і інженерних кадрів, гранична фізична і моральна зношеність основних фондів, згортання державної підтримки науки і базисних інновацій, втрата стратегічного мислення і настроїв серед ділової еліти — все це впливає на послаблення позицій України для самостійного науково-технологічного прориву до світових ринків високих технологій.

Для виправлення ситуації особливе значення матиме пряме залучення вітчизняної науки до формування найважливіших сфер життя країни, всього державного апарату до реалізації економічної і науково-технічної політики (стандартизація, організація держзамовлень, входження в цільові науково-технічні програми, регіональна політика, спеціальні економічні пільги і санкції і т.д.) і боротьби з потенційними конкурентами (знов-таки стандартизація, економічний протекціонізм, складність митних процедур і режимних обмежень, тиск на пресу, виробників і споживачів і т.д.).

Сьогодні правомірно стверджувати: чим потужнішими інформаційними можливостями володіє держава, тим вірогідніше (за інших умов) вона може домогтися стратегічних переваг. У цьому контексті стають зрозумілими оцінка інформації військово-політичним керівництвом США як стратегічного ресурсу і причини постійного збільшення асигнувань на розвиток і вдосконалення інформаційних технологій.

Так, якщо у США в 1980 році на придбання інформаційних технологій витрачалось близько 8 млрд. дол., то в 1998 році — вже понад 30 млрд. Причому фінансування статті на придбання інформаційних технологій вийшло на перше місце серед усіх програм озброєнь США (далі йдуть ракетно-ядерні, космічні програми і т. д.). Аналогічна картина спостерігається в Німеччині, Японії, Франції.

Слід зазначити, що політична ситуація, що склалася у світі в результаті припинення «холодної війни» між Заходом і Сходом, не торкнулася такого її атрибуту, як розвідка. Провідні західні країни продовжують модернізувати і розвивати свої розвідувальні служби, вдосконалювати технічну розвідку, нарощувати її можливості. Усе це відбувається на тлі розширення можливостей розвідки в зв'язку з проведенням інспекцій при

реалізації міжнародних договорів, створенням спільних підприємств, скороченням районів і територій із регламентованим відвідуванням їх іноземцями. Поряд із традиційними пріоритетами технічних розвідок у сферу їхнього інтересу все більшою мірою втягуються питання технологій, фінансів, торгівлі, ресурсів, доступ до яких відкривається в зв'язку з конверсією, розвитком міжнародних інтеграційних процесів, широким упровадженням комп'ютерних технологій.

У цих умовах сліпе наслідування рішень, які виправдали себе в минулому, неодмінно призвело б до шкоди державним інтересам у військовій, політичній, економічній та інших сферах. Час вимагає вдосконалення як сформованої системи захисту інформації в організаційному плані, так і концептуальних, методологічних підходів до захисту інформації, оскільки:

- інформаційні технології принципово змінили обсяг і важливість інформації, що обертається в технічних засобах її передавання і обробки;

- відійшла в минуле фактична державна монополія на інформаційні ресурси, зокрема, набуло конституційного закріплення право громадянина шукати, одержувати і поширювати інформацію;

- старий адміністративний механізм управління захистом інформації став і неможливим, і неефективним, тоді як необхідність міжвідомчої координації у сфері захисту інформації об'єктивно зросла;

- завершилася гостра військово-політична конфронтація між СРСР і країнами НАТО, контрольоване скорочення озброєнь, що почалося, і розвиток заходів довіри у військовій галузі поставили вимогу забезпечити розумне поєднання відкритості і заходів, спрямованих на захист державної таємниці;

- у зв'язку з поглибленням процесу включення країни у міжнародний поділ праці, зміцненням економічних, культурних, гуманітарних контактів з іншими державами багатобіжних — обмежувальних заходів, що застосовувалися для захисту інформації, стали неприйнятними.

Світ вступив у еру інформаційного суспільства, і перед Україною постало завдання озброїти державний апарат доброякісною інформацією, і чим обширнішою і доступнішою вона буде, тим менше витратиться на побудову і порівняння різнома-

нітних варіантів рішень у галузі економічного управління, де відповідальні рішення, а відтак, їх наслідки, що мають велике значення для майбутнього, потребують урахування безлічі факторів і їхніх взаємозв'язків.

Концепт інформаційної політики був би неповним, якби ми вивели за межі розгляду погляди фахівців на серйозні проблеми інформаційної війни та інформаційної боротьби в сучасному світі, бо ХХІ століття, на жаль, не принесло людству миру. Навпаки, держави дедалі частіше застосовують військову силу для розв'язання світових проблем, набирає обертів міжнародний тероризм, набуваючи форм глобального явища і активно використовуючи у своїх цілях новітні інформаційні технології.

Розвиток інформаційних технологій, досягнення людства в галузі обчислювальної техніки, нове розуміння стратегічної ролі інформаційних ресурсів у цілому і науково-технічного доробку зокрема, вже на початку формування у провідних країнах світу інформаційного суспільства спонукали до докорінного перегляду концепцій і положень у сфері збройної боротьби. Враховуючи, що воєнна сфера завжди була головним споживачем досягнень науково-технологічного прогресу і основним замовником науково-технічних програм, а також те, що саме в ній упроваджуються найновітніші інформаційні технології, ми не можемо обійти увагою нині існуючих у світі поглядів фахівців на інформаційну війну та інформаційну боротьбу — без цієї підмножини наш концепт інформаційної політики в сучасному світі був би неповним. Зробимо це, посилаючись на підходи до розв'язання цих проблем у США, КНР та Росії.

1.3. ІНФОРМАЦІЙНЕ ПРОТИБОРСТВО І НАЦІОНАЛЬНА БЕЗПЕКА У ХХІ СТОЛІТТІ

1.3.1. Погляди фахівців США на сутність інформаційної війни та інформаційної боротьби

1.3.1.1. Місце і роль інформаційного протиборства в забезпеченні національних інтересів США

Виступаючи перед працівниками Центрального розвідувального управління в штаб-квартирі ЦРУ в Ленглі, Президент США Джордж Буш назвав головні загрози безпеці Сполучених

Штатів — на другому місці, після тероризму, в цьому переліку він зазначив інформаційну війну, і вже за нею — поширення зброї масового ураження і засобів її доставки³⁹.

Як вважають американські військові фахівці, до порядку денного поставлене питання про перенесення акценту в збройному протиборстві з традиційних його форм ведення (вогнь, удар, маневр) в інформаційно-інтелектуальну й інформаційно-технічну сфери, тобто туди, де ведеться підготовка, відбувається прийняття і реалізація воєнних і політичних рішень. Майбутня війна може бути спровокована в інформаційній сфері й охоплюватиме всю сукупність завдань у політичній, економічній, технічній і воєнній галузях.

За свідченням документів Об'єднаного штабу Комітету начальників штабів (ОШ КНШ) ЗС США, інформаційна війна може вестися як у воєнний, так і в мирний час, як на державному (дипломатичні, економічні, інформаційні, спеціальні та інші сили і засоби), так і на військовому рівнях (силами і засобами боротьби із системами бойового управління).

Хвиля «цифрової революції» створила абсолютно новий економічний сектор, якого раніше не було, що спровокувало зростання інтенсивності конфліктів з метою захоплення й утримання переваги в даному секторі нової світової економіки. Капіталом, що відіграє чільну роль у «цифровій революції», є інтелектуальний капітал насамперед у галузі інформаційних технологій.

Основний продукт цього сектору — інформація, інформаційні ресурси — мають унікальні властивості, які не властиві іншим секторам економіки: на відміну від усіх інших ресурсів інформація придатна для багаторазового використання і для численних користувачів. При цьому чим більше вона використовується, тим вартіснішою вона стає. Те саме можна сказати про мережі, що зв'язують різні джерела інформації.

Одночасно з переходом від постіндустріального до інформаційного суспільства нового значення набуває і споконвічна боротьба щита і меча, броні й снаряда. Полем бою в конфліктах ХХІ століття стає віртуальний кіберпростір, у якому розгортаються дії інформаційних воєн, а процеси глобалізації накладають певний відбиток і на модернізацію основних концепцій воєнної стратегії ХХІ століття, що переконливо підтверджує побудова нової національної воєнної стратегії США.

Ряд офіційних документів, таких як доповідь Міністерства оборони США «Report of the quadrennial Defense Review», концептуальний документ Комітету начальників штабів «Joint Vision 2010», доповідь комісії з національної оборони «Transforming Defense National Security in the 21st Century, Report of the National Defense Panel» констатують відповідно: «Ми визнали, що світ продовжує швидко змінюватися. Ми не в змозі цілком зрозуміти чи передбачити проблеми, що можуть виникнути у світі за часовими межами, зумовленими традиційним плануванням. Наша стратегія приймає такі невизначеності і готує збройні сили таким чином, щоб справитися з ними»; «Прискорення темпів змін робить майбутні умови більш непередбачуваними і менш стабільними, висуваючи широкий діапазон вимог до наших сил»; «Проблеми ХХІ століття будуть кількісно і якісно відмінними від тих, котрі були характерні для періоду «холодної війни», у зв'язку з чим виникне потреба докорінної зміни інститутів національної безпеки, воєнної стратегії і підходів до питань оборони до 2020 року»⁴⁰.

Незважаючи на невизначеність загроз, що постають, і проблем ХХІ століття, США мають намір і в майбутньому зберегти роль світового лідера. Для цього вони орієнтуються на випереджальне формування адекватного їхнім інтересам стратегічного середовища, а у разі неуспіху — на готовність до силової нейтралізації несприятливих для них процесів.

Так, у серпні 1997 році ЦРУ провело брифінг про розвиток Каспійського регіону як одного з найбагатших на нафтові і газові ресурси. Для спостереження за розвитком політичних подій у регіоні й оцінки його потенціалу ЦРУ створило спеціальний підрозділ. Після доповіді представника ЦРУ присутня на брифінгу тодішній держсекретар США Мадлен Олбрайт заявила, що «одним із найважливіших завдань буде робота над формуванням майбутнього цього регіону». У цих словах — суть інформаційної війни: створення всіма способами необхідної, що відповідає глобальній стратегії США, політичної атмосфери в тих регіонах, що, як вони вважають, належать до сфери їхніх національних інтересів. Зазначимо, що силове вирішення питання при цьому вважається провалом і має використовуватися тільки в крайньому випадку.

Така концепція може бути реалізована, наприклад, як стратегія «керованого хаосу», що ґрунтується, як у випадку з Югославією, на міжетнічних чи міжрелігійних конфліктах. Прояви такої політики спостерігаються і на Кавказі, і в Криму, і в Білорусі.

У колах деяких фахівців термін «інформаційна війна» тлумачиться як відкритий і/чи прихований цілеспрямований інформаційний вплив систем одна на одну з метою одержання певного виграшу в матеріальній сфері. Однак інформаційна війна не є простим «впливом систем одна на одну». В основних документах Збройних сил США говориться, що інформаційний вплив має різнобічний характер і змінюється залежно від розв'язуваних завдань і обстановки. Він може бути інформаційно-розвідувальним (виявлення військового, економічного, політичного і культурного потенціалу); полягати в протидії будь-яким видам розвідки супротивника (OPSEC); спотворювати, руйнувати, нейтралізовувати, знищувати чи, навпаки, захищати інформацію (CNA, CND); займатися комп'ютерним відтворенням реальної чи віртуальної неадекватної обстановки і візуалізації на полі бою; здійснювати інформаційно-психологічний (PSYOP) чи легальний і нелегальний фізичний вплив на особовий склад, об'єкти, бойову техніку, зброю, лінії зв'язку і управління; зосереджуватися на демонстративних діях, обмані і введенні в оману (Military Deception); одержати завдання на радіоелектронне придушення; застосовуватися для зниження помітності об'єктів, бойової техніки і зброї; захисту особового складу, об'єктів, бойової техніки, зброї, органів управління і різних радіоелектронних засобів від впливу на них електромагнітного чи інших видів спрямованої енергії; відведення самонавідної зброї від найбільш важливих цілей тощо. В основі такого впливу — насамперед психологічні і світоглядні фактори, а також комп'ютерні технології. Було б хибно зводити його до класичної спецпропаганди — у це поняття закладений значно ширший зміст.

У документах ОШ КНШ ЗС США також зазначається, що на державному рівні основними завданнями інформаційної війни є:

- примушення військово-політичного керівництва ворожих і союзних держав до прийняття політичних рішень, що забезпечують інтереси США;

- забезпечення національної безпеки США;

- здобування інформації, необхідної для прийняття військово-політичних рішень.

Так, наприкінці 1996 року на одному із симпозіумів Роберт Банкер представив доповідь, присвячену новій військовій доктрині Збройних сил США XXI століття (концепції «Force XXI»). Ключовим моментом у ній є поділ усього театру воєнних дій на дві складові — традиційний простір і кіберпростір, причому останньому надається більш важливого значення. Банкер запропонував доктрину «кіберманевру», що має з'явитися природним доповненням до наявних воєнних концепцій, що мають на меті нейтралізацію чи придушення збройних сил супротивника (концепції «Force XXI»).

Отже, до сфер ведення бойових дій, крім землі, моря, повітря і космосу, тепер включається й інфосфера, і, як підкреслюють військові експерти, основними об'єктами поразки в нових війнах будуть інформаційна інфраструктура і психологія супротивника (з'явився навіть термін «human network»).

Таким чином, під інформаційною війною (Information Warfare, IW) мається на увазі комплексний вплив на систему державного і військового управління конфронтуючої сторони, на її військово-політичне керівництво. У принципі цей вплив має ще в мирний час приводити до прийняття сприятливих для країни — ініціатора інформаційного тиску рішень, а в ході конфлікту цілком паралізувати функціонування інфраструктури управління супротивника.

Інформаційна війна складається з дій, які починаються для одержання інформаційної переваги в забезпеченні національної воєнної стратегії, що досягається шляхом впливу на інформацію й інформаційні системи супротивника з одночасним зміцненням і захистом власної інформації й інформаційних систем та інфраструктури.

Здатність не тільки реагувати, а й передбачати проблеми до того, як вони досягнуть кризової точки, — це те, що прагнуть набути США в найближчому майбутньому. При цьому вони віддають пріоритет системам і засобам, що дають змогу різко зменшити ще на початковій стадії конфлікту (чи й до його початку) функціональні можливості протидії держави-супротивника шляхом проведення наступальних інформаційних операцій.

Інформаційна перевага фахівцями США тлумачиться як здатність збирати, обробляти і розподіляти безупинний потік інформації про ситуацію, перешкоджаючи супротивнику зробити те саме. Вона може бути також визначена і як здатність призначити і підтримувати такий темп проведення операції, що перевершує будь-який можливий темп супротивника, надаючи йому можливість домінувати протягом усього часу її проведення, залишаючись непередбачуваним, і діяти, випереджаючи супротивника в його відповідних акціях.

Подібна перевага дає змогу мати реальне уявлення про бойову обстановку і надає інтерактивну і високоточну картину дій супротивника і своїх військ у реальному масштабі часу. Інформаційна перевага є інструментом, що забезпечує командуванню можливість застосовувати у вирішальних операціях широко розосереджені побудови різнорідних сил, підвищувати захист своїх військ і вводити в бій угруповання, склад яких максимальною мірою відповідає завданням, а також здійснювати гнучке і цілеспрямоване матеріально-технічне забезпечення.

Інформаційна війна припускає проведення заходів, спрямованих проти систем управління і прийняття рішень (Command&Control Warfare), а також проти комп'ютерних й інформаційних мереж і систем (Computer Network Attack, CNA). Деструктивний вплив на системи управління і прийняття рішень досягається за допомогою психологічних операцій (Psychological Operations, PSYOP), спрямованих проти персоналу й осіб, які приймають рішення й впливають на їхню моральну стійкість, емоції й мотиви прийняття рішень; практичних кроків по оперативному і стратегічному маскуванню (OPSEC), дезінформації і фізичному руйнуванню об'єктів інфраструктури.

Концепція інформаційної війни передбачає:

- знешкодження (у воєнний час) елементів інфраструктури державного й воєнного управління (ураження центрів командування й управління);
- електромагнітний вплив на елементи інформаційних і телекомунікаційних систем (радіоелектронна боротьба);
- одержання розвідувальних даних у результаті перехоплення і дешифрування інформаційних потоків, переданих по каналах зв'язку, а також по побічних випромінюваннях і шля-

хом спеціального впровадження технічних засобів перехоплення інформації;

— здійснення несанкціонованого доступу до інформаційних ресурсів (завдяки використанню програмно-апаратних засобів прориву систем захисту інформаційних і телекомунікаційних систем супротивника) з наступним їхнім перекручуванням, знищенням чи викраданням або порушення нормального функціонування цих систем;

— формування і масове поширення по інформаційних каналах супротивника чи глобальних мережах дезінформації або тенденційної інформації для впливу на оцінки, наміри й орієнтацію населення й осіб, що приймають рішення;

— одержання інформації шляхом перехоплення й обробки відкритої інформації, переданої по незахищених каналах зв'язку, циркулюючої в інформаційних системах, а також друкованої у відкритому порядку у ЗМІ.

Основними об'єктами впливу в інформаційній війні є:

- особовий склад;
- мережі зв'язку й інформаційно-обчислювальні мережі, використовувані державними організаціями при виконанні своїх управлінських функцій;
- воєнна інформаційна інфраструктура, що вирішує завдання управління військами;
- інформаційні і керуючі структури банків, транспортних і промислових підприємств;
- засоби масової інформації (передусім електронні).

У принципі про будь-яку систему, здатну за своїми вхідними даними відпрацьовувати той чи інший алгоритм, можна говорити як про інформаційну систему — об'єкт інформаційної війни.

Ряд фахівців зазначає, що застосування інформаційної зброї — це технологія, що охоплює:

- аналіз способів і механізмів активізації в конкретній системі супротивника, закладених у неї програм;
- пошук програми самознищення;
- розробка конкретної інформаційної зброї;
- застосування інформаційної зброї по заданому об'єкту.

Оскільки інформаційна війна пов'язана з питаннями інформації і комунікацій, то це є війна за знання — за те, кому

швидше і точніше стануть відомі відповіді на запитання: що, і коли, де, чому і наскільки надійним вважає окремо взята країна і її армія свої знання про себе і своїх супротивників. При цьому засобом ведення інформаційної війни «інформаційною зброєю» є саме використання інформації і пов'язаних з нею технологій для впливу на воєнні і цивільні системи супротивника.

Відповідно до статутів американських ЗС на них покладені такі завдання у сфері інформаційної війни:

- примушувати військово-політичне керівництво ворожих держав приймати рішення, що забезпечують створення вигідних для ЗС США умов;
- завоювати й утримати «інформаційну перевагу» над супротивником;
- досягати цілей і вирішення завдань кампаній і операцій;
- здобувати і вчасно оновлювати інформацію для прийняття воєнних рішень.

ЗС США використовують такі сили і засоби боротьби із системами бойового управління (БСБУ), всебічно забезпечені розвідкою і контррозвідкою: радіоелектронну війну (EW), воєнну дезінформацію (MD), оперативну безпеку (OPSEC), психологічні операції (PSYOP), фізичну поразку, захоплення і виведення з ладу (PD), атаки і захист комп'ютерних мереж (CNA,CND).

Залежно від театру війни, оперативної обстановки і кола розв'язуваних завдань будь-яка складова цих сил може відіграти вирішальну роль.

Інформаційна операція розглядається як комплекс заходів щодо маніпулювання інформацією з метою досягнення й утримання переваги шляхом впливу на інформаційні процеси в системах супротивника, з тим уточненням, що інформаційні системи розглядаються в широкому плані, а не тільки в технічному аспекті, вони включають і державу, суспільство в цілому.

Командування ЗС США на основі вивчення досвіду локальних конфліктів останнього десятиліття дійшло висновку, що інформаційні операції можуть бути ефективними тільки при комплексному й інтегрованому використанні всіх сил і засобів, які залучаються для ведення інформаційної війни.

За ступенем ефективності інформаційних операцій командування ЗС США виділяє *три рівні об'єднаності сил і засобів БСБУ*.

Низький рівень — характеризується загальними оперативними завданнями, але розрізненим використанням в операції сил і засобів БСБУ (наприклад, «Буря в пустелі»). Такі інформаційні операції американські фахівці називають «особливими операціями» чи «спеціалізованими бойовими діями».

Високий рівень — характеризується не тільки загальними оперативними завданнями, а й єдиним плануванням, взаємопроникненням і злиттям сил і засобів БСБУ — такі операції дістали назву «синергетичних» (системне планування і застосування сил і їхня інтеграція).

Найвищий рівень об'єднаності сил і засобів БСБУ може бути досягнутим при чіткому виконанні ряду умов: загальні оперативні цілі і завдання, повний взаємозв'язок усіх сил і засобів БСБУ, забезпечення єдності ритмів, темпів і взаємного доповнення у використанні сил і засобів БСБУ і розвідки на всіх етапах операції і на всю її глибину, іншими словами, здійснюється своєрідне злиття всіх сил БСБУ за місцем, часом, завданнями, напрямками і темпами їхнього ведення. Такі інформаційні операції названі «когерентними» операціями ЗС США ХХІ століття.

Відмітною особливістю інформаційних операцій є приділення значної уваги заходам з «оперативної безпеки» (Operational Security), яку не слід ототожнювати з поняттями «стратегічне маскування» і «оперативне маскування», прийнятими в Збройних Силах України. По-перше, OPSEC за своєю суттю означає протидію усім видам розвідки (в усіх сферах). По-друге, OPSEC здійснюється під безпосереднім керівництвом командирів не тільки на стратегічному й оперативному рівнях, а й на низовому тактичному рівні. По-третє, ставляться такі основні завдання оперативної безпеки, як:

- інформаційна безпека;
- безпека органів і систем управління, а також систем і засобів автоматизації управління",
- фізична безпека особового складу ЗС (організація пропускового режиму, роботи з документами, охорона життєдіяльності, бойової роботи й ін.);
- безпека об'єктів, бойової техніки і зброї;
- розробка способів протидії розвідці супротивника, виявлення демаскуючих ознак, каналів витоку інформації, контроль

і оповіщення ЗС про критичну інформацію, що могла стати відомою супротивнику.

Воєнна дезінформація у ЗС США (Military Deception) відповідно до американських статутів за масштабом застосування має чотири рівні — стратегічний, оперативний, тактичний і видовий (в інтересах одного виду ЗС) — і передбачається при організації БСБУ, проведенні інформаційних операцій для оперативної безпеки, радіоелектронної війни і психологічного впливу.

Варто сказати кілька слів і про зміст терміна «електронна війна» (Electronic Warfare) чи, точніше, «радіоелектронна війна» та його зв'язок з термінами «радіоелектронна боротьба» і «радіоелектронна протидія». Відповідно до єдиного статуту ОШ КНШ ЗС США радіоелектронна війна, яка є основою БСБУ, являє собою комплекс заходів щодо використання випромінювань електромагнітного й іншого видів спрямованої енергії, самонавідної на випромінювання радіоелектронних засобів (РЕЗ) зброї, а також засобів радіоелектронного захисту і радіоелектронного забезпечення бойових дій. Об'єкти впливу і захисту для радіоелектронної війни (на відміну від радіоелектронної боротьби й електромагнітного впливу) — це не тільки радіоелектронні засоби, а й особовий склад ЗС (передусім органів управління), бойова техніка, об'єкти, зброя і комп'ютерні мережі. З'явилися нові засоби її ведення (легальні і нелегальні).

Упродовж десяти років у ЗС США визначилися *оперативно-тактичні тенденції розвитку радіоелектронної війни*, до яких можна віднести такі, як:

- поетапна докорінна зміна змісту, цілей, завдань, форм і способів її ведення (радіоелектронні контрзаходи, радіоелектронні контрконтрзаходи, заходи радіоелектронного забезпечення, що у ході розвитку були складовою частиною заходів боротьби із системами зв'язку і управління; радіоелектронна атака);
- радіоелектронний захист: радіоелектронне забезпечення бойових дій, що ввійшли сьогодні до складу заходів боротьби із системами бойового управління;
- використання для ведення радіоелектронної війни нових видів випромінювань електромагнітної і спрямованої енергії;
- розширення кількості об'єктів впливу і захисту (особовий склад ЗС, бойова техніка, об'єкти, зброя, комп'ютерні і різні інформаційні мережі);

— повна інформатизація й автоматизація процесів (не тільки радіоелектронної війни, а й БСБУ в цілому);

— зміщення акцентів впливу і захисту в інформаційно-інтелектуальну сферу, в сферу підготовки, прийняття і реалізації воєнних рішень, особливо в першій фазі проведення операцій;

— жорсткий взаємозв'язок, взаємозалежність, взаємний вплив усіх елементів радіоелектронної війни і БСБУ на основі єдиних оперативних цілей і завдань, при постійній координації всіх зусиль у ході проведення операції.

Виникли *нові форми ведення радіоелектронної війни*: радіоелектронний удар, радіоелектронно-вогневий удар, інформаційно-радіоелектронна блокада та ін.

Ряд експертів підкреслює, що ефективність стримування й інших стратегічних концепцій значною мірою залежить від здатності США впливати на сприйняття і рішення урядів інших країн. Під час криз інформаційні операції можуть допомогти стримати супротивника від проведення акцій, що заподіюють збитків США та їх союзникам.

Слід також зазначити, що в американській воєнній термінології вживається поняття «*інформаційне забезпечення*» як складовий елемент розвідувального забезпечення операції чи бою (Electronic Warfare Support), що є одним із нових елементів «радіоелектронної війни».

Отже, роблять висновок фахівці, на національно-стратегічних і воєнно-стратегічних рівнях як інформаційні операції в мирний час, так і інформаційні бойові дії в кризові чи конфліктні періоди потребують високого ступеня координації дій між урядовими структурами, включаючи Міністерство оборони.

Нова *проблема* полягає в *інтеграції інформаційних впливів у загальну стратегію національної безпеки*. Експертами США відзначається необхідність розробки єдиної концепції інформаційної війни, що включає як воєнний, так і фінансовий, торговий, психологічний, юридичний та інші аспекти. Зауважимо, що при цьому головна стратегічна мета наступальних інформаційних дій зміщується з активного впливу на автоматичні системи і засоби озброєнь на особистість, тобто на людину, яка приймає рішення. На думку експертів, такі дії можуть бути найбільш ефективними в мирний час і на початкових етапах зародження конфлікту, що добре узгоджується з основними цілями національної політики безпеки США.

Прогнозуючи стратегічні умови до 2020 року, американські військові експерти виявили і зафіксували в офіційних документах ряд основних тенденцій світового розвитку, що висувають перед США потенційні проблеми. Уточнюється, що висновки, базовані на прогнозі тенденцій розвитку, можуть бути відносно точними тільки для найближчого часу (від одного року до трьох років), але їхня точність зменшується в міру віддалення в майбутнє. Цілком зрозуміло, що деякі тенденції (наприклад, демографічні) можуть бути відстежені з високою мірою вірогідності. Інші ж (типу геополітичних) менш передбачувані. Вони піддані значно більш швидким змінам під впливом різних подій.

Військові аналітики США роблять загальний висновок: держави хоча і залишаються домінантними одиницями міжнародної системи, але чим далі підпадатимуть під вплив зростаючої могутності багатонаціональних корпорацій і міжнародних організацій. На цей фактор звертають увагу у своїх працях і українські фахівці⁴¹. Розвиток технологій, геополітична трансформація, демографічний «тиск», а також посилення економічних і соціальних тенденцій можуть радикально змінити реалії сьогодення. Діапазон можливих сценаріїв широкий, і їх складно (чи неможливо) передбачити. Отже, центральною проблемою для оборонної структури є розвиток у тому напрямі, що дасть їй змогу ефективно реагувати на будь-який варіант подій. Це диктує необхідність постійної адаптації до дедалі нових тенденцій.

Можливості засобів інформаційної війни постійно зростають. Однак спинимося тільки на вузькій частині ймовірних впливів, що дістала назву «атаки на комп'ютерні мережі» (Computer Net-work Attack). У рамках цього обмеження будемо розуміти, що *інформаційна зброя* являє собою сукупність спеціально організованої інформації, інформаційних технологій, що дає змогу цілеспрямовано змінювати (знищувати, спотворювати), копіювати, блокувати інформацію, переборювати системи захисту, обмежувати допуск законних користувачів, здійснювати дезінформацію, порушувати функціонування носіїв інформації, дезорганізовувати роботу технічних засобів, комп'ютерних систем і інформаційно-обчислювальних мереж.

За даними американських експертів, нині у більш як 25 країнах світу ведуться розробки по створенню засобів ведення кібернетичних комп'ютерних воєн.

Засоби, використовувані як інформаційна зброя, називаються засобами інформаційного впливу (ЗІВ) чи засобами спеціального програмно-математичного впливу (ЗСПМВ). За метою використання інформаційну зброю поділяють на забезпечувальну й атакуючу.

Забезпечувальною називається інформаційна зброя, застосовувана проти засобів захисту інформації системи, що атакується. До її складу належать засоби комп'ютерної розвідки і засоби подолання системи захисту.

Особлива роль приділяється використанню атакуючої інформаційної зброї, призначення якої — впливати на збережену, оброблювану і передану в системі інформацію. Вона охоплює чотири, основних види засобів інформаційних впливів:

- засоби порушення конфіденційності інформації;
- засоби порушення цілісності інформації;
- засоби порушення доступності інформації;
- засоби психологічних впливів на абонентів інформаційної системи.

У сукупності застосування цих засобів спрямоване на зрив виконання інформаційною системою цільових завдань. За способом реалізації інформаційну зброю можна розподілити на три великих класи: математична (алгоритмічна), програмна й апаратна.

Інформаційна зброя, що належить до різних класів, може застосовуватися спільно, деякі її види можуть мати риси кількох класів.

Відповідь на питання питань військово-політичного керівництва США — як забезпечити «тотальне панування» у ХХІ столітті — можна знайти в документах Комітету начальників штабів Joint Vision 2010 й Joint Vision 2020 (травень 2000 рік), які розкривають погляди правлячих кіл Сполучених Штатів Америки. У них насамперед йдеться про завоювання інформаційної переваги над ймовірним супротивником, про прагнення переконати увесь світ у правильності своїх дій у мирний час і показати свою рішучість у випадку війни, щоб забезпечити свою перевагу в будь-яких конфліктах.

Відповідно до цих документів основною складовою кардинального підвищення бойових можливостей збройних сил є досягнення інформаційної і технологічної переваги, що змінить

сучасне уявлення про маневр, удари, захист і тилове забезпечення і призведе до появи нових оперативних концепцій пануючого маневру, високоточного бою, цілеспрямованого тилового забезпечення і всеосяжного захисту. У них зосереджена увага на трьох основних факторах, що мають стати основою успіху в реалізації цих концепцій:

- забезпечення тісної і повної взаємодії ЗС США та їхніх союзників;

- новаторство в усіх сферах, розробка і використання нових способів ведення бойових дій з метою підвищення бойових можливостей «об'єднаних сил» (у тому числі інформаційно-психологічних й інформаційно-технічних);

- упередження супротивника в прийнятті і реалізації політичних і воєнних рішень, досягнення й утримання над ним інформаційної переваги.

Реалізація розглянутих концепцій, на думку експертів, дасть можливість проводити рішучі операції за обставин, тобто досягти тієї якості, що в документі «Єдина перспектива 2010» визначається як «тотальне панування». Воно виступає, якщо говорити про США в цілому, національною метою інформаційного домінування стосовно будь-якої ворожої національної чи транснаціональної спільноти. Щодо Міністерства оборони США, то воно спрямовує свої дії інформаційної системи для театру воєнних дій (ТВД), яка дасть змогу, на думку Пентагона, забезпечувати військових інформацією такого рівня і якості, що не були доступні раніше.

Заплановані на рівень 2010 року характеристики інформаційної системи для театру воєнних дій дадуть споживачам можливість одержати набагато якіснішу його візуалізацію (як за часом, так і в просторі) і забезпечити концентрацію зусиль розосереджених підрозділів на розв'язуваних завданнях. Очікується, що така інформаційна система, інтегрована з комунікаційних мереж і мереж датчиків, програмного забезпечення й організаційних структур, надасть:

- надійний і якісний зв'язок для підрозділів;
- оперативну інформацію про хід операції;
- точні і своєчасні розвідувальні дані про місце розташування і дії противника;

- каталог баз даних щодо зони операції і можливостей супротивника, а також доступ до цих баз;

- точне розміщення дружніх сил і їхній бойовий статус (у реальному часі);

- здатність проведення операцій на всьому ТВД, виконуваних безупинно з розосереджених місць проектування сили;

- роботу в реальному часі інформації, що надає загальну картину ситуації, яка складається на ТВД;

- вбудовані можливості самозахисту (з багаторівневим захистом доступу), що дають змогу розподіляти інформацію серед організацій, союзників, неурядових організацій.

Інформаційні системи театру воєнних дій — це сукупність підсистем для збирання, обробки, аналізу, архівування і розподілу інформації, що, власне, і покликані забезпечити досягнення інформаційної переваги над супротивником. При зосередженні на наявному чи потенційному супротивнику інформаційні системи, що збирають дані, охоплюють відкриті джерела, традиційну розвідку, системи спостереження і виявлення. Зібрані дані стають інформацією після їхньої обробки і приведення до вигляду зручного для користування. Для задоволення специфічних запитів споживача така інформація може трансформуватися в розвідувальну в разі застосування до неї цілеспрямованого аналізу, інтерпретації, звіряння з іншою інформацією та загальним інформаційним контекстом.

В епоху становлення інформаційного суспільства багато в чому змінився характер стратегічної розвідки. Тепер на розвідувальні служби покладений як основний обов'язок, крім випереджального оповіщення вищого керівництва країни про можливу агресію, і завдання по досягненню інформаційної переваги над супротивником. Як розвиток засобів ведення комп'ютерної розвідки останнім часом згадується віртуальна архітектура об'єднаної розвідувальної інформації (Joint Intelligence Virtual Architecture, **JIVA**), що надає можливість перерозподілити технічні і програмні ресурси та формувати «віртуальне розвідувальне робоче середовище», особливий підпростір у інформаційному просторі. У ньому здійснюється скоординований перегляд, узгодження, затвердження і розподіл кінцевої розвідувальної продукції.

Однією з головних передумов реалізації своєї інформаційної переваги США вважають технологічне випередження в галузі інформатизації. Водночас військові аналітики США констатують, що сучасні інформаційні технології доступні кожному, хто має фінансові можливості. Постійно зростаючі поширення і доступність інформації створюють для потенційного супротивника (за зростаючої залежності США від інформації й інформаційних систем) передумови досягнення тимчасового локалізованого паритету чи асиметричної переваги в бойовому просторі. Швидко впровадження перспективних технологій робить ймовірнісною несподівану появу асиметричних загрозливих можливостей у широкого кола потенційних супротивників. Очікується, що рівень інтенсивності інформаційних операцій, проведених супротивником і в мирний час, зросте з ескалацією кризової ситуації.

США планується, що до 2010 року збройні сили одержать у розпорядження інтегровану архітектуру прийняття рішень, що базується на штучному інтелекті, нанотехнологіях, ефективному синтезі інформації, багатофункціональних процесорах зі здатністю підтримувати прийняття рішень у реальному часі, технологіях стискання даних для підвищення швидкості обробки. При цьому використання командуванням інформаційних систем з підключенням установок штучного інтелекту як операційних посилювачів ефективності бойових дій вплине на доктрину, організацію і навчання збройних сил. Зокрема, моделюючи установки нададуть можливість в інтегрованому й інтерактивному режимі прогнозувати варіанти дій, змінювати їхню тактику, приймати рішення і діяти.

Здобуваючи ефективні наступальні (як правило, превентивні) й оборонні інформаційні можливості, США, природно, прагнуть не тільки захистити свої системи від «кібернетичних атак», а й швидко знаходити їхнє джерело і давати адекватну «відповідь» на будь-якому рівні дій, але до його фізичного знищення.

Технологічні досягнення, що дають багато переваг, таять у собі також і можливу вразливість — за відсутності систематичних пророблень їхнього застосування. Так, зростаючі можливості систем обробки інформації можуть викликати перенасиченість даними. Щоб уникнути цієї небезпеки, пропонуються технології штучного інтелекту, які вбудовані в системи підтримки прийняття рішень і допомагають подолати інформаційне пе-

ревантаження. Проте американські фахівці відзначають, що здатність індивідуального рішення є унікальною людською рисою, яку не можуть замінити навіть найбільш досконалі системи підтримки. Ключ до рішення — систематично розробляти, використовуючи нові підходи в навчанні, здатність людини приймати правильні рішення у швидко мінливій комп'ютеризованій обстановці, що відбиває розподілені театри воєнних дій.

Лунають застереження, що надмірна надія на інформаційні системи може перешкоджати прийняттю рішень чи стримувати їх, а також збільшувати «час на міркування». Варто також враховувати, що ускладнені інформаційні системи мають більший ризик виходу з ладу. Тому підготовка і вольові якості персоналу, незалежно від технологічних вдосконалень, як і раніше вимагають неослабних зусиль і продовжують залишатися основою майбутніх воєнних операцій.

Отже, перехід інформації в розряд найважливіших ресурсів людства і виникнення проблеми володіння цим ресурсом, зумовлює перегляд основних стратегічних концепцій ведення бойових дій у XXI столітті. Стає цілком зрозуміло, що інформаційна перевага буде головною складовою майбутньої воєнної стратегії подібно до того, як на початку XX століття такими складовими з'явилися панування в повітрі і масоване застосування бронетанкової техніки.

Перемогу у воєнних діях у XXI столітті визначатимуть уже не стільки технічні засоби озброєнь, скільки інформація. Це ще раз підтверджує ті принципи розбіжності, які треба буде пройти людству при переході від постіндустріального суспільства до суспільства інформаційного.

1.3.1.2. Роль засобів масової інформації у збройних конфліктах

Ерік Повел (інформаційний офіс Нідерландів у НАТО), виступаючи в Москві на конференції з основних напрямів воєнного будівництва в європейських країнах, організаторами якої були Міжнародний інститут стратегічних досліджень (Лондон) спільно з Міжрегіональним суспільним фондом підтримки воєнної реформи, відзначив, що в даний час виграти кампанію в ЗМІ так само важливо, як перемогти у воєнній операції⁴². По-перше, це

забезпечує підтримку громадської думки, по-друге, ти переко-нуєш супротивника, що не маєш наміру здаватися.

Під час кризи в Косові НАТО діяло на п'яти «фронтах»: воєнні операції Об'єднаних сил; політичні і дипломатичні зусилля для розв'язання кризи; перша гуманітарна інтервенція в Албанії; інформаційна війна; «війна» усередині НАТО.

Варто відзначити, з якими ж «зовнішніми» проблемами зіткну-лися прес-служби НАТО.

1. Високі суспільні очікування «чистої, високотехнологічної війни». НАТО скинуло 23 тис. бомб, з яких тільки близько 30 не вразили намічених цілей. Це — одна десята відсотка, колись не досяжна міра точності. Але ЗМІ і громадська думка в цілому були шоковані: вони ігнорували 99,9% успішних дій, а з 0,1% промахів зробили центральну драму і мірило оцінки воєнної і моральної ефективності дій НАТО.

2. Цензура Белграда.

3. Важливий урок, що в даний час вивчається в НАТО, по-лягає в тому, що ЗМІ зацікавлені в новинах, причому в яскра-вих, підкріплених «картинкою». Представник НАТО щодня вит-рачав тисячі слів, щоб роз'яснити, що відбувається, але словам не вірили, тому що не були подані фотосвідчення.

4. Конфлікт відбивався ЗМІ як серія окремих яскравих інци-дентів, при цьому губився загальний контекст, фундаменталь-на динаміка. Люди були недостатньо поінформовані про дипло-матичні і політичні зусилля.

Ерік Повел також охарактеризував деякі внутрішні пробле-ми прес-центру альянсу:

1. НАТО допустило політичний прорахунок, тому що біль-шість дипломатів очікували, що Милошевич здасться через кілька днів бомбардувань. У результаті прес-операція НАТО не була підготовлена до тривалого конфлікту.

2. Виявилось важким доставляти швидко інформацію з ТВД у Брюссель, щоб надати штаб-квартирі НАТО можливість швид-ко відповідати на запитання преси.

3. Координація спілкування з пресою в столицях країн — членів НАТО теж виявилася нелегкою справою, що іноді при-зводило до того, що чиновники в столиці Х говорили не те, що чиновники в столиці У. Зосередившись на країнах — членах

НАТО, ми дещо упустили з вигляду громадську думку і ЗМІ в деяких ключових державах-партнерах у регіоні.

Усе це призвело до перегляду тактики щодо ЗМІ в сере-дині квітня 1999 року. Після трагічного інциденту в Дьяковиці, коли літаки альянсу помилково скинули бомби на конвой з біжен-цями, убивши приблизно 15 осіб, було прийняте рішення про створення Центру операцій ЗМІ в штаб-квартирі НАТО. Центр об'єднав офіцерів, відповідальних за зв'язок із пресою, з інши-ми співробітниками, насамперед з висококваліфікованими політич-ними і військовими представниками країн НАТО. Вони готували матеріал для щоденних брифінгів прес-секретаря альянсу.

Ключові функції військових прес-центрів, як вважається в НАТО, мають полягати в тому, щоб домагатися:

— тісної координації всіх ліній ЗМІ і деконфліктизації новин («витоку») серед головних членів НАТО (щоденні прес-конфе-ренції);

— тіснішої і швидшої координації й обміну інформацією з військовим штабом і командуванням, що діють на головному напрямку;

— ясного і масового моніторингу й аналізу (включаючи теле-бачення Росії і Сербії);

— дослідження і збору інформації для забезпечення можли-вості висвітлювати події дня;

— підготовки спростувань і відповідей на критичні запитання і текстів промов для міністрів і генерального секретаря НАТО;

— надання кваліфікованого персоналу для ведення інформа-ційних операцій.

Уроки ж, що прес-служби НАТО винесли зі свого спілку-вання з пресою під час операції, такі:

1. Не слід розраховувати на ідеальні відносини зі ЗМІ. У конфлікті завжди буде опонент, а це означає, що доведеть-ся мати справу з певною кількістю пропаганди, дезінформації і простих контраргументів. Нарешті, ЗМІ віддають перевагу «про-мовляючим головам» — відставним генералам, ученим, що зав-жди стверджують, що володіють досконалішою стратегією, що відсутність постійного успіху означає поразку. Під час кризи і конфлікту відносини НАТО з пресою неминуче будуть важчи-ми, ніж у мирний час, тому інформаційна стратегія НАТО має

бути спрямована на оптимальне надання основних аргументів і цілей НАТО й оптимальне відображення критики з боку ЗМІ.

2. Необхідно підсилювати підрозділи НАТО по зв'язках із пресою з моменту, коли втручання НАТО в конфлікт виявиться неминучим. Прес-служба НАТО укомплектована для нормальних мирних операцій. Очевидно, що вона потребуватиме швидкого посилення для висвітлення подій глобального значення, тому потрібно якомога швидше створити щось на зразок Центру в Косові.

3. Слід поліпшити надання воєнної інформації. На початку повітряної кампанії проти Югославії НАТО критикували в пресі не стільки за заподіяні збитки, скільки за неточності й затримки з роз'ясненням того, що відбувається. У НАТО зрозуміли: коли не вдається пояснити інцидент через відсутність інформації, історія обігрується ЗМІ кілька днів, але коли подавали інформацію швидко, історія зникала з новин майже одразу ж.

4. Треба більше знати про свого супротивника. Збігло кілька тижнів, щоб знайти людей, які розбираються в югославських справах. Крім того, для прес-служб має бути більше доступної розвідінформації. Надто часто повторювалося таке: коли знаходилася цікава інформація, прес-службам НАТО говорили, що вона засекречена і не може використовуватися відкрито. Необхідно також спробувати донести свої повідомлення до населення супротивника. Були ідеї про створення радіостанції, що веде мовлення на Югославію, а також про використання літаків для передавання радіопрограм, але вони так і не матеріалізувалися до кінця кампанії.

5. В епоху телебачення «картинка» відіграє вирішальну роль. Преса часто більше вірила «картинкам» Милошевича, ніж словам НАТО. Тому в альянсі задумуються над тим, що потрібно вчасно надавати наочні фотосвідчення на підтримку висунутих обвинувачень (палаючі будинки, масові поховання і т. д.)

6. Оволодіння медійним простором у НАТО оцінюється як погана робота. Брифінги проводилися в штаб-квартирі НАТО вранці і вдень, брифінг влаштовувався в МО в Лондоні під час ленчу, брифінг у Вашингтоні — по вечорах. Тим самим створювалася така ситуація, коли жоден телеглядач у світі не міг одержати послання від НАТО, водночас важливо постійно надавати ЗМІ свіжу інформацію.

«Чи були наші інформаційні операції успішними?» — запитує представник прес-служби НАТО. І сам же відповідає на нього: «Що стосується країн НАТО, то відповідь позитивна. Люди, природно, не відчували великого ентузіазму, але вони здебільшого вірили, що наші дії були виправдані. По-друге, чи переконали ми свого супротивника? Явно що так, оскільки, зрештою, Милошевич здався. Я сподіваюся, що наші інформаційні зусилля теж відіграли в цьому деяку роль. По-третє, чи переконали ми жертв, тобто косівських албанців? Так, люди говорили нашому прес-секретарю Шеа, що прес-конференції НАТО переконали їх не впадати у відчай».

1.3.1.3. Погляди військового керівництва США на ведення інформаційної війни

У обстановці, що склалася, ряд розвинутих західних держав, передусім США, на початку 1990-х років безпосередньо приступили до вивчення і пророблення проблем, пов'язаних із протиборством у інформаційній сфері, чи так званою інформаційною війною (ІВ). За твердженням американських фахівців, окремі положення концепції «інформаційна війна» уже протягом тривалого часу реалізуються США на політичному рівні переважно у формі психологічної війни, що була використана для розвалу СРСР і Організації Варшавського Договору⁴³.

У США під цим терміном розуміється комплексний вплив на систему державного і військового управління конфронтуючої сторони, її політичне і військове керівництво, яке вже в мирний час приводило б до прийняття сприятливих для Сполучених Штатів рішень, а в ході війни цілком паралізувало структуру управління супротивника. Водночас з наступальним впливом інформаційне протиборство передбачає забезпечення надійного захисту національної інформаційної інфраструктури США.

У даний час розроблена Пентагоном концепція ведення ІВ реалізується на двох рівнях: державному й воєнному.

На державному рівні мета інформаційного протиборства в широкому розумінні полягає в ослабленні позицій конкуруючих держав, підриві їхніх національно-державних підвалин, порушенні системи державного управління шляхом інформаційного впливу на політичну, дипломатичну, економічну і соціальну

сфери життя суспільства, проведення психологічних операцій, підривних та інших деморалізуючих пропагандистських акцій.

Інформаційні операції (ІО) на цьому рівні можуть вирішувати завдання захисту національних інтересів США, запобігання міжнародним конфліктам, припинення провокаційних і терористичних акцій, а також забезпечення безпеки національних інформаційних ресурсів.

На воєнному рівні ІО являють собою комплекс заходів, проведених у масштабах збройних сил країни, їхніх видів, об'єднаних командувань у зонах, і є складовою частиною воєнних кампаній (операцій). Вони спрямовані на досягнення інформаційної переваги над супротивником (насамперед в управлінні військами) і захист своїх систем управління. Для цього можуть використовуватися будь-які наявні військові і технічні сили і засоби за формального дотримання правових, моральних, дипломатичних, політичних і воєнних норм. Перед збройними силами вперше поставлено завдання впливу на супротивника ще в загрозливий період (до початку активних бойових дій) для того, щоб забезпечити вигідну для США спрямованість процесів управління й прийняття рішень конфронтуючою стороною.

Такий розподіл завдань, за оцінкою американських експертів, має забезпечити необхідну ефективність проведення заходів у рамках інформаційного протиборства, що в теорії і практиці воєнного будівництва в Сполучених Штатах стало розглядатися як особлива форма міждержавних відносин після аналізу підсумків війни в зоні Перської затоки. У грудні 1992 року основні положення концепції інформаційного протиборства стосовно діяльності ЗС були сформульовані в загальному вигляді в директиві міністра оборони США № TS 3600.1 «Інформаційна війна». У ній ставилися завдання Об'єднаному штабу КНШ і штабам видів збройних сил по розробці нової концепції. Ця робота була завершена до кінця 1993 року і знайшла своє відображення в директиві голови КНШ МОР № 30-93. У ній ідеї інформаційного протиборства були трансформовані для ЗС у концепцію «боротьби із системами управління» (БСУ). У директиві КНШ БСУ визначалася як «комплексне проведення за єдиним задумом і планом психологічних операцій, заходів щодо оперативного маскування, радіоелектронної боротьби і фізич-

ного знищення пунктів управління і систем зв'язку з метою позбавлення супротивника інформації, виведення з ладу чи знищення його систем управління при одночасному захисті своїх від аналогічних дій». Складові інформаційного протиборства наведені на рис. 2.

Директива МОР № 30-93 фактично виділила боротьбу із системами управління в самостійний вид оперативного забезпечення бойової діяльності військ. Теорія боротьби із системами управління дістала свій подальший розвиток в Єдиному статуті КНШ № 3-13.1 1995 року «Спільні дії різнорідних сил по боротьбі із системами управління супротивника».

Надалі, в міру розвитку комп'ютерних технологій і в зв'язку з тенденціями підвищення ролі інформації в усіх сферах життя сучасного суспільства, у тому числі у воєнній справі, американське командування було змушене ширше поглянути на проблему інформаційного протиборства.

У документі КНШ ЗС США «Єдина перспектива — 2010», який визначив основні напрями розвитку оперативно-стратегічних концепцій застосування збройних сил у XXI столітті, підкреслювалося, що *головною рисою збройної боротьби в наступному столітті буде переміщення акценту в сферу інформаційного протиборства і досягнення «інформаційного панування», що стане обов'язковою умовою перемоги над будь-яким супротивником*. Такі самі положення містить і випущений у 2000 році черговий документ КНШ «Єдина перспектива — 2020».

Подальшого розвитку концепція інформаційного протиборства набула в інструкції КНШ 3210.01 А «Концепція інформаційних операцій об'єднаних угруповань збройних сил» від 1996 року, Єдиному статуті КНШ № 3-13 «Доктрина спільних дій по проведенню інформаційних операцій», директивах, статутах і настановах штабів видів збройних сил 1998-го.

Поняття інформаційних операцій є ширшим, ніж боротьба із системами управління, БСУ, але не замінює його. Завдання БСУ як самостійного виду бойового забезпечення — боротьба із системами управління і зв'язку як з цільовими об'єктами, а мета проведення ІО — вплив на інформаційні системи супротивника і циркулюючу в них інформацію чи знищення їх. При організації інформаційних операцій дії по БСУ централізовано інтегруються в них і стають їх невід'ємними елементами.

I I i . и И .
! : : И !
^o ^{• — П} ¹ ^{§•} ^ı ^ı ^ı
Л Н и Ј ђ п Н Й љ і І
І І І І І Н Г И Л В і <
і і й і й ! ! і
U If Lyj гЧ^п | ЦГТ] І

•.....І.....

У наведених документах визначені цілі, завдання й основні принципи інформаційного протиборства, обов'язки керівних органів і посадових осіб по їхній організації і плануванню в мирний час і в умовах кризової обстановки. Крім того, у них перераховані вимоги щодо розвідувального забезпечення інформаційних операцій, а також до підготовки особового складу, який забезпечує їхнє планування і проведення.

Військове керівництво США вважає, що *ефективне інформаційне протиборство має забезпечити командирам (командуючим) можливість нав'язати конфронтуючій стороні помилкове бачення обстановки, примусити її до ведення воєнних дій у не вигідних для неї умовах.* Це досягається переважно шляхом проведення комплексу заходів, що дають змогу, з одного боку, порушити процес прийняття рішень супротивником, а з іншого — обробляти інформацію по циклу прийняття рішень у своїй системі управління ефективніше і швидше, ніж це може зробити командувач конфронтуючого угруповання військ.

Практична реалізація концепції інформаційного протиборства здійснюється шляхом проведення Ю, які є комплексом заходів, що мають на меті вплинути на інформацію й інформаційно-управляючі системи (ІУС) супротивника при одночасному захисті своєї інформації й інформаційних систем. Вони є важливим чинником у досягненні й утриманні інформаційної переваги в ході операцій об'єднаних угруповань ЗС. ІВ являє собою відповідну операцію, проведену в період кризової ситуації чи конфлікту (включаючи війну) для досягнення специфічних цілей над специфічним супротивником чи супротивниками. Стосовно інформаційних операцій термін «супротивник» розглядається у ширшому розумінні. Під ним маються на увазі організації, групи осіб чи окремі особи, що приймають рішення або здійснюють дії, спрямовані на зрив виконання завдань, поставлених перед командуванням об'єднаних збройних сил.

Підготовка і проведення інформаційних операцій пов'язані з узгодженням і розв'язанням на рівні національного військово-політичного керівництва країни комплексу питань законодавчого і політичного характеру. ІО проводяться на всіх рівнях воєнних дій, межі між якими найчастіше мають умовний характер.

На *стратегічному рівні* такі операції проводяться за рішенням військово-політичного керівництва країни і покликані забезпечити досягнення національних стратегічних цілей. Під час них здійснюється вплив на всі елементи державного устрою потенційних супротивників (політичні, воєнні, економічні й інформаційні) при одночасному захисті своїх державних структур. Для досягнення цілей Ю на цьому рівні має забезпечуватися високий ступінь координації між військовими органами й урядовими закладами і відомствами США, а також союзниками та партнерами по коаліції.

На *оперативному рівні* ІО проводяться для забезпечення успішного ходу операції чи кампанії в цілому чи вирішення головних завдань операції. Їх мета — вплив на лінії зв'язку, системи тилового забезпечення і бойового управління збройними силами супротивника при одночасному захисті аналогічних систем як своїх ЗС, так і союзників. Інформаційні операції, проведені на цьому рівні, можуть сприяти досягненню стратегічних цілей.

Ю на *тактичному рівні* проводяться з метою забезпечення вирішення тактичних завдань. Вони зосереджені на впливі на інформацію й інформаційні системи, такі як системи зв'язку, бойового управління, розвідки й інші, що безпосередньо забезпечують ведення бойових дій з'єднаннями і частинами супротивника при одночасному захисті як систем своїх, так і союзників.

В основу концепції інформаційного протиборства закладена обопільна залежність (уразливість) США та їхніх потенційних супротивників від інформації й інформаційних систем. У зв'язку з цим при її реалізації розглядаються два аспекти діяльності — вплив на інформаційну інфраструктуру супротивника і захист свого власного інформаційного середовища. Відповідно всі 10 поділяються на наступальні й оборонні.

Наступальні інформаційні операції являють собою комплексне проведення за єдиним задумом і плану заходів щодо оперативного маскування, радіоелектронної боротьби, програмно-математичного впливу на ІУС, фізичного знищення (виведення з ладу) об'єктів інформаційної інфраструктури, а також психологічних і спеціальних Ю. *Оперативне маскування поєднує такі прийняті у воєнній термінології ЗС США окремі поняття, як введення супротивника в оману і забезпечення прихованості*

діяльності військ (сил). У ході таких операцій здійснюються заходи, що справляють вплив на свідомість людей і спрямовані на зрив процесу прийняття рішень, а також дії з метою порушення роботи чи знищення елементів інформаційної інфраструктури. Новим елементом наступальних інформаційних операцій порівняно з концепцією боротьби із системами управління є спеціальні ІО і заходи щодо програмно-математичного впливу на комп'ютерні мережі супротивника.

Оборонні інформаційні операції являють собою взаємозалежні процеси по захисту інформаційного середовища, розкриттю ознак нападу, відновленню боєздатності й організації відповідних дій на агресію (напад). Їхніми основними елементами є:

- забезпечення фізичної безпеки інформаційної інфраструктури, безпеки інформації й прихованості дій військ (сил);
- розкриття заходів щодо оперативного маскування супротивника; контрпропаганда;
- контррозвідка; радіоелектронний захист і спеціальні інформаційні операції.

Оборонні ІО мають забезпечувати своєчасність і точність передачі даних, гарантований доступ до них користувачів в умовах інформаційного впливу супротивника. У їх ході передбачається проведення заходів щодо відновлення боєздатності інформаційних систем.

Наступальні й оборонні ІО можуть проводитися за єдиним задумом і планом і взаємно доповнювати одна одну. Вони орієнтовані на ті самі об'єкти впливу, якими можуть бути:

- органи управління держави і її збройних сил;
- ІУС цивільної інфраструктури (телекомунікаційні, включаючи засоби масової інформації, транспортні, енергетичного комплексу, фінансового і промислового секторів);
- керуючі елементи воєнної інфраструктури (системи зв'язку, розвідки, бойового управління, тилового забезпечення, управління зброєю;
- лінії, канали зв'язку і передачі даних;
- інформація, яка циркулює чи зберігається в системах управління;
- суспільство в цілому (як цивільне населення, так і особовий склад збройних сил), його державні, економічні та соціальні інститути;

— керівний склад і персонал автоматизованих систем управління, які беруть участь у прийнятті рішень.

У період проведення миротворчих операцій об'єктами впливу можуть бути також воєнізовані, партизанські і політичні організації, релігійні і соціальні групи, окремі особи, які відкрито чи таємно виступають проти присутності Збройних сил США чи союзників, перешкоджаючи виконанню ними своєї місії.

Ефект цільового інформаційного впливу на супротивника, за оцінками американських експертів, можна порівняти з застосуванням засобів масового ураження (ЗМУ), і загроза піддатися такому впливу може стати важливим фактором стримування потенційного агресора. На їхню думку, ефективність цієї загрози прямо пропорційна рівню технологічного розвитку і масштабам використання комп'ютерної техніки в системах управління країною. Як комплексний процес інформаційна операція являє собою інтегроване, узгоджене за часом використання різних засобів і методів, орієнтованих на досягнення визначеної загальної мети.

Основу досить багатого і постійно удосконалюваного арсеналу методів ведення інформаційної війни ЗС США становлять як історично добре перевірені заходи, пов'язані з використанням традиційних видів оперативного (бойового) забезпечення військ (сил), так і новітні способи подібного впливу на супротивника.

При проведенні наступальних інформаційних операцій основними традиційними методами є психологічні операції і заходи щодо оперативного маскування, які здавна застосовувалися для впливу на свідомість людей у процесі прийняття ними рішень, а також такі дії, як радіоелектронне придушення і використання засобів фізичного знищення, спрямовані на порушення функціонування чи знищення елементів інформаційної інфраструктури. До новітніх методів у даному разі можна віднести програмно-математичний вплив на комп'ютерні мережі супротивника і спеціальні інформаційні операції. Є також безліч інших способів і дій, що можуть інтегруватися при проведенні різного роду операцій. Деякі з них мають наступальний характер, інші — оборонний. На думку американських фахівців, їх спільне використання дуже важливе для досягнення успіху в ході проведення як оборонних, так і наступальних операцій.

Психологічні операції являють собою заходи щодо поширення спеціально підготовленої інформації з метою здійснення впливу на емоційний стан, мотивацію й аргументацію дій, прийняття рішення і поведінку окремих керівників, організацій, соціальних чи національних груп і окремих осіб іноземних держав у бажаному для США і їхніх союзників напрямі. Вони можуть бути стратегічними, оперативними і тактичними за своїми масштабами, і їхнє проведення може забезпечуватися заходами оперативного маскування.

На стратегічному рівні психологічні операції можуть проводитися у формі пропаганди певних політичних чи дипломатичних позицій, офіційних заяв або повідомлень керівників держави.

На оперативному рівні такі операції можуть проводитися у вигляді поширення листівок, за допомогою радіо- і телемовлення, ведення мовлення з використанням засобів гучномовного зв'язку, а також інших засобів для передавання інформації, що містить заклики, які спонукають особовий склад збройних сил супротивника до масового саботажу, дезертирства, втечі або капітуляції.

На тактичному рівні проведення психологічних операцій передбачає використання гучномовного зв'язку й інших засобів для нагнітання страху, розпалення пристрастей і зростання непокори в рядах супротивника.

Вплив на політичних і військових лідерів, а також на керівників (найбільш помітних представників) ЗМІ, культури і мистецтва конфронтуючої сторони є важливим аспектом інформаційного протиборства в цілому і психологічних операцій зокрема. У зв'язку з цим у США особлива увага приділяється створенню колективних і індивідуальних моделей поведінки представників вищої і середньої ланки державного і воєнного керівництва, зокрема складанню психологічних портретів на керівників (у військах — до командира з'єднання включно).

Для вивчення воєначальників потенційного супротивника і складання їхніх психологічних портретів широко використовуються відкриті джерела, агентурні дані, а також заходи в рамках військового обміну, масштаби якого військово-політичне керівництво США наполегливо прагне розширити.

Заходи щодо оперативного маскування проводяться під керівництвом командувачів об'єднаних угруповань військ (сил).

їхнім змістом є здійснення впливу на органи прийняття рішень супротивника через його системи збору, аналізу і розподілу інформації шляхом надання їм свідомо хибної інформації і приховування ознак реальної діяльності військ (сил). Мета цих заходів полягає в тому, щоб заплутати, дезінформувати розвідувальні органи супротивника, змусити їх робити неправильні висновки і, як наслідок, спонукати військове керівництво супротивника до помилкових дій. Ці заходи дають також змогу випередити супротивника в прийнятті рішення, що є ключем до успіху будь-якої операції.

Оперативне маскування передбачає застосування таких способів, як:

- дезінформація — поширення свідомо хибної інформації про склад, стан, дислокацію, боєздатність своїх військ, їхні угруповання, характер і спосіб вирішення завдань, плани-призначення і стан військової техніки та об'єктів;

- імітація — відтворення правдоподібних демаскуючих ознак, характерних для реальної діяльності військ (об'єктів), створення радіоелектронної обстановки з використанням імітаторів, радіотехнічних пристроїв, несправжніх споруджень і об'єктів, макетів військової техніки і т.д.;

- демонстративні дії — навмисна демонстрація перед супротивником спеціально виділеними силами і засобами активної діяльності з метою його дезорієнтації і приховування справжніх намірів організаторів;

- забезпечення прихованості дій — визначення ознак, які розпізнаються розвідувальними системами супротивника і дають йому змогу на основі їхнього аналізу одержувати особливо важливу і своєчасну інформацію; вибір і проведення заходів, які забезпечували б приховування цих ознак і тим самим знижували б до прийняттого рівня уразливість союзників від дій розвідки супротивника.

Заходи щодо оперативного маскування звичайно проводяться одночасно з іншими заходами, які забезпечують дії об'єднаних сил. Планування цих заходів здійснюється згори донизу для того, щоб плани по введенню супротивника в оману підпорядкованих ланок підтримували і забезпечували аналогічні плани командування. У вищій за належністю ланці воно припускає використання частин і підрозділів найнижчого рівня, хоча самі

їхні командири і їхні безпосередні начальники можуть не знати змісту загального плану заходів. Тому в таких випадках важливою є координація планів заходів щодо введення супротивника в оману командирів нижчих за належністю частин і підрозділів старшим начальником.

Успіх проведення заходів щодо оперативного маскування визначальною мірою залежить від ефективності розвідувального забезпечення. Розвідка в цьому випадку здійснює розкриття об'єктів супротивника, щодо яких плануються ці дії, надає допомогу в розробці правдоподібної версії, запропонованої для дезінформації, виборі найбільш перспективних об'єктів для реалізації дезінформації й оцінює ефективність проведених заходів.

Радіоелектронна боротьба поділяється на радіоелектронне придушення, радіоелектронний захист і радіоелектронне забезпечення. Радіоелектронне придушення являє собою дії наступального характеру, які здійснюються з метою дезорганізувати, нейтралізувати чи знизити можливості супротивника, спрямовані на ефективне використання ним радіоелектронних систем у різних ланках управління збройних сил. Радіоелектронний захист передбачає такі дії, як захист радіоелектронних засобів (РЕЗ) від перешкод, створюваних противником, і здійснення контролю (спостереження) за роботою РЕЗ союзників, з метою усунення їх взаємного впливу один на одного. Радіоелектронне забезпечення являє собою дії, спрямовані на виявлення, ідентифікацію і визначення місцезнаходження РЕЗ противника, які можуть бути як джерелами отримання розвіданих, так і джерелами інформаційних загроз.

При прийнятті рішення про використання засобів радіоелектронного придушення враховуються не лише цілі кампанії чи операції, а й ризик від можливих дій противника у відповідь. Для досягнення максимального ефекту операції обов'язковою умовою є тісна координація сил і засобів РЕВ з іншими заходами щодо забезпечення інформаційних операцій, здійснюваних розвідкою і зв'язком.

Фізичне знищення елементів інформаційної інфраструктури розглядається як здійснювані в ході ІО дії по застосуванню засобів вогневої поразки і фізичного знищення з метою виведення з ладу ключових елементів системи управління і зв'язку противника.

Програмно-математичний вплив на комп'ютерні мережі (комп'ютерна атака) визначається як дії з застосуванням апаратно-програмних засобів, спрямовані на використання, спотворення, підміну чи знищення інформації, що міститься в базах даних комп'ютерів й інформаційних мереж, а також на зниження ефективності функціонування або виведення з ладу самих комп'ютерів і комп'ютерних мереж.

Способи програмно-математичного впливу з цілком зрозумілих причин не є надбанням широкого загалу гласності й описуються в спеціальній грифованій літературі, призначеній для обмеженого кола зацікавлених осіб. Що стосується засобів такого впливу, а роботи в галузі їхнього створення ведуться в США з 1990 року, то їх можна розподілити на такі:

- «логічні бомби» — приховані управляючі програми, що за визначеним сигналом чи у встановлений час вводяться в дію, знищуючи або спотворюючи інформацію, забороняючи доступ до тих чи інших важливих фрагментів керованого інформаційного ресурсу або дезорганізуючи роботу технічних засобів. В АСУ військами і зброєю подібне втручання навіть протягом короткого проміжку часу може докорінно вплинути на хід і результат бою, операції;

- комп'ютерні віруси, що являють собою спеціалізовані програмні продукти, здатні відтворювати «логічні бомби» (що мають при цьому ще більшу руйнівну силу) і впроваджувати їх дистанційно в інформаційні мережі супротивника. Крім того, вірусам властиво самостійно розмножуватися, тобто копіювати себе на магнітних носіях;

- програмні продукти на кшталт «троянського коня» — програми, впровадження яких дає змогу здійснювати прихований несанкціонований доступ до інформаційного масиву супротивника для добування розвідданих;

- нейтралізатори текстових програм, що забезпечують збереження природних і штучних недоліків програмного забезпечення;

- навмисно створені, приховані від звичайного користувача інтерфейси для входу в систему. Вони, як правило, свідомо вводяться в програмне забезпечення програмістами-розроблювачами з корисливими чи диверсійно-підливними цілями;

- малогабаритні пристрої, здатні генерувати електромагнітний імпульс високої потужності, що забезпечує виведення з ладу радіоелектронної апаратури.

Крім того, значна увага приділяється створенню нових засобів впливу на системи зв'язку, збирання й обробки інформації. Так, з початку 1990-х років здійснюється перехід до використання не виявлюваних перешкод інтелектуального впливу (блокування ключових елементів повідомлення, наприклад, назв і координат пунктів, часу дії з одночасним введенням хибних ключових елементів). Такі системи базуються на автоматизованому аналізі структури повідомлень, відстеженні ключових слів, синтезуванні мови в реальному масштабі часу.

До дій, що забезпечують проведення інформаційних операцій, відносять і заходи щодо організації зв'язку з цивільною адміністрацією і населенням, а також по зв'язку з громадськістю, здійснювані відповідними службами збройних сил.

Підрозділи по зв'язку з цивільною адміністрацією безпосередньо орієнтовані на дії, що забезпечують взаємну підтримку при проведенні психологічних операцій.

Декларативно завдання служби по зв'язках із громадськістю полягають у тому, щоб: оперативно доводити точність і своєчасність інформації про здійснювану кампанію (операцію) до зацікавлених організацій і громадськості; роз'яснювати цілі і завдання, здійснювані збройними силами; надавати командуванню каналів ЗМІ для інформування супротивника (потенційних супротивників) про наміри і можливі дії союзних військ. При цьому стверджується, що всі ці дії не можуть застосовуватися для введення супротивника в оману чи для дезінформації громадськості. На практиці, однак, можливості цієї служби широко використовуються для формування міжнародної громадської думки у вигідному для США дусі шляхом вибіркового і дозованого подання інформації.

У цілому концепція інформаційного протистояння в тому вигляді, в якому вона реалізується у ЗС США, не є новим поняттям для вітчизняного воєнного мистецтва. Теоретичні основи інформаційного протистояння досить повно розкриті у вітчизняній воєнній науці через поняття «боротьба із системами управління супротивника», «радіоелектронна війна», «завоювання

ня панування в ефірі», «психологічна війна», «дезінформація», «воєнна хитрість» і т.п. «Новизна» американського підходу до теорії інформаційного протиборства полягає в комплексному використанні військово-теоретичних розробок з цієї тематики і своїх технологічних досягнень у галузі інформатики.

У даний час США, володіючи значною перевагою в галузі розробки і використання новітніх радіоелектронних систем і комп'ютерних технологій і ґрунтуючись на постулатах нової концепції, прагнуть закріпити за собою домінуючу роль не тільки в політичній, економічній і військовій сферах, а й у світовій інформаційній інфраструктурі.

1.3.2. Інформаційна війна за поглядами військових аналітиків Китаю

1.3.2.1. Інформаційне протиборство у збройній боротьбі

Як вважають китайські військові аналітики, майбутня війна може бути спровокована збоєм у комп'ютерних мережах промислового сектору світової економіки і являтиме собою, власне, безкомпромісну боротьбу в інформаційній сфері. Така війна охопить усю сукупність воєнних, політичних і економічних аспектів життєдіяльності людей. На першому плані в ній виявляться інформаційні системи.

Люди, що беруть участь в інформаційній війні, за своїм становищем аж ніяк не солдати (не носять військової форми, не стріляють), однак вони можуть приймати стратегічні рішення як персонал так званих мозкових центрів, основа яких — фахівці найвищої кваліфікації в галузі інформаційних технологій (IT). Якнайшвидша мобілізація особового складу збройних сил у період розвитку конфліктів утрачає свою актуальність. Замість цього передбачається «мобілізація» інформаційних центрів і вступ їх у війну першими.

Вплив на супротивника може здійснюватися опосередковано, наприклад через Інтернет. У цьому випадку протиборствующій стороні не завжди вдасться визначити, що це — несанкціонований доступ в інформаційну мережу комп'ютерного хакера чи підступ ворога? Такий характер дій передбачає наявність у

кожного «комп'ютерного солдата» високого рівня незалежності й ініціативи. Він спроможний працювати самостійно, без взаємодії з ким-небудь і вводити в інформаційні мережі супротивника таку величезну кількість марних відомостей, що через перевантаження каналів зв'язку блокується нормальна робота інформаційних систем останнього, знижується імовірність відповідних дій. Таким чином, активно поєднуючи людський і штучний інтелект, використовуючи вмілу організацію, можна ввергнути супротивника в стан інформаційного хаосу.

Крім того, передбачається докорінна зміна традиційних форм і способів збройної боротьби, затвердження пріоритету концепції інформаційної війни і т.д. Інформаційні технології — це ключ до оволодіння всіма іншими технологіями світу, який стрімко розвивається, і оскільки вони поступально соціалізуються, а сфери зіткнення інтересів людей дедалі більше розширюються, то ведення інформаційного протиборства перестало бути заняттям суто збройних сил.

У даний час новітні концепції ведення операцій швидко завоюють собі право на життя. Інформація вже сама по собі не тільки своєрідна зброя, а і цінний трофей. Якість, кількість і швидкість її передавання є ключовими елементами інформаційної переваги. За своїм впливом на об'єкт її можна порівняти з високоточною зброєю і засобами ведення електронної війни. Інформаційна зброя може використовуватися для нанесення втрат як активним, так і пасивним системам упізнання супротивника, з найбільшою ефективністю виводити з ладу його бойові засоби, приводитися в дію після певного «інкубаційного» періоду. Тому надійний захист інформації, своєчасне прийняття контрзаходів щодо нейтралізації негативного впливу є основними пунктами підготовки і ведення інформаційної війни.

Отже, в інформаційне століття засоби і методи, концепції ведення війни докорінно змінюються. Протиборство воюючих сторін може мало вплинути на зовнішній матеріальний світ, викликавши руйнування інформаційних мереж. Шантаж й інші ефективні заходи активного характеру, застосовувані за допомогою інформаційного впливу, дають можливість істотно послабити супротивника чи завдати йому поразки. Кривавий характер війни змінюється безкровною конфронтацією інформаційних систем. Ігнорування питань інформаційної війни в да-

ний час є неприпустимим, інакше легко опинитися на задвірках історичного процесу.

Незважаючи на відсутність загальноприйнятого офіційного визначення поняття «інформаційна війна», китайські військові експерти вже давно оперують ним. У цьому питанні вони широко використовують наробітки зарубіжних, зокрема американських, військових фахівців. При цьому вони виділяють шість аспектів у змісті цього поняття: розвідка військового, економічного, політичного і культурного потенціалу супротивника і блокування аналогічних дій з його боку; руйнування (придушення) інформаційної складової його систем бойового управління і зв'язку і захист своєї; забезпечення безперешкодного доступу до глобальних інформаційних систем і недопущення до них супротивника; широке використання АСУ як засобу інформаційного забезпечення будь-яких видів бойової діяльності; створення гнучкої і мобільної бази даних; комп'ютерне відтворення реального поля бою. Вважається, що інформаційна війна включає також бойові дії за участю сучасних інформаційно насичених засобів ведення бою. Передбачається створення спеціальних бойових формувань, призначених для захоплення і контролю інформації, застосування усіх видів інформаційної зброї, придушення (нейтралізації) інформаційних систем супротивника, введення його в оману і протидії йому.

Військові аналітики КНР, формулюючи поняття «інформаційна війна», тлумачать його у вузькому і широкому сенсах. *У вузькому розумінні інформаційна війна — це польова інформаційна війна, тобто бойові дії в сфері управління військами.* Сюди входять активне використання засобів розвідки, заходи щодо введення супротивника в оману й оперативного маскування, психологічні операції, послідовна поразка його інформаційних систем, систем бойового управління і зв'язку, а також дії щодо захисту своїх аналогічних систем.

У широкому розумінні інформаційна війна — ще великомасштабні бойові дії з перевагою інформаційної складової, які характеризуються застосуванням спеціально призначених для її ведення військових формувань, оснащених високоточною зброєю. Якщо основним засобом досягнення успіху на полі бою в ХХ столітті були танки, то в майбутньому ним стане комп'ютер.

Це у свою чергу передбачає застосування комп'ютерних вірусів, здатних руйнувати програмне забезпечення технічних засобів органів бойового управління і зв'язку, ініціювати збої в системах управління і наведення високоточної зброї і тим самим значно зменшувати бойовий потенціал супротивника. Війна із широким використанням високоточної зброї зажадає істотного збільшення швидкості добування розвідданих, часу попередження про удари супротивника, поліпшення взаємодії командирів усіх щаблів, підвищення маневреності військ, а відтак, і ефективності усіх видів інформаційного забезпечення. Літаки, танки, кораблі і ракети, виготовлені з застосуванням технології «Стелт», стануть основною бойовою технікою військ. Бойові дії з їхньою участю радше нагадуватимуть змагання у швидкості виявлення і знищення та характеризуватимуться високою інтенсивністю і швидкоплинністю.

Китайські військові експерти пильну увагу приділяють зарубіжним розробкам у сфері ведення інформаційної війни. Як і західні військові фахівці, вони вважають, що інформаційна війна не є в буквальному розумінні війною на полі бою, підготовкою до якої є численні навчання і маневри військ. Збройні конфлікти останнього часу спонукали їх виділити *кілька характерних рис, притаманних інформаційній війні.*

По-перше, «прозорість» поля бою. Звична «гарячка бою» поступається місцем «хірургічним» методам роботи підрозділів інформаційної війни. Оператор комп'ютера може здійснювати безупинний контроль за ситуацією, спостерігати відображуване на дисплеї розташування своїх військ і військ супротивника, його об'єкти, концентрацію і переміщення його сил.

По-друге, *загальна координація дій військ* за допомогою створення єдиного каналу управління для всіх бойових підрозділів і підрозділів тилового забезпечення. Усі оперативні функції зазначених формувань (розвідка, управління, зв'язок) у цьому випадку зводяться в єдину систему. Наприклад, оператор інформаційного центру, маючи дані про кількість, склад і координати виявлених цілей супротивника, робить розрахунки для їх розподілу за засобами поразки, визначає кількість необхідних боєприпасів і т.д.

По-третє, *ведення бойових дій у реальному масштабі часу*, тобто негайне реагування на зміну бойової обстановки. ,

По-четверте, *точність ударів*, що вирізняються своєрідною чистотою й акуратністю, подібною до роботи скальпеля хірурга.

Для перемоги в інформаційній війні виникає потреба оснащення збройних сил передовими інформаційними технологіями.

Такі збройні сили являють собою нову категорію військ із самостійною теорією ведення бойових дій, особливо організаційно-штатною структурою, високим рівнем підготовки особового складу й озброєнням, що цілком відповідають вимогам інформаційної війни. Китайські військові експерти скрупульозно переймають досвід зарубіжних колег у цій галузі. Особливо пильну увагу вони приділяють дослідженням у США — єдиній країні, де план створення армії нового типу вже існує не тільки на папері, а й поступово втілюється в життя.

Бойові формування, призначені для ведення інформаційної війни, використовуватимуть технології цифрового зв'язку, цілісну систему розвідки і бойового управління, високоточну зброю. Їхній арсенал поповнять радары нового покоління, системи впізнання типу «свій — чужий», елементи глобальних навігаційних систем. Досвід навчань, проведених армією США, свідчить, що сучасні ІТ забезпечують, наприклад, скорочення середнього часу підльоту бойових вертольотів і підготовки їх до атаки цілі з 26 до 18 хвилин, збільшення відсотка цілей, в які влучають, з 55 до 90. Обробка і передача повідомлень у вищестоящі штаби в ланці «рота — батальйон» скорочується з 9 до 5 хвилин.

Для пристосування до потреб інформаційної війни організаційно-штатна структура збройних сил зазнає змін: чисельність сухопутних військ скорочуватиметься, а ВМС і ВПС — зростатиме. Можливо, з'являться нові види збройних сил, такі як космічні сили й інформаційно-комп'ютерні війська. Збільшиться кількість офіцерів-професіоналів, особливо з інженерною освітою. Організація частин і підрозділів ґрунтуватиметься на оптимальній комбінації високоосвіченого особового складу і високотехнологічної техніки; управління має стати ще гнучкішим.

На думку керівництва КНР, її збройні сили спроможні адекватно реагувати на зміни, що відбуваються в сфері світового військового будівництва. Поки що за розробками й оснащенням сучасним озброєнням вони відстають від розвинутих країн За-

ходу. Однак китайські військові експерти вважають, що у світлі майбутніх збройних конфліктів, зокрема з застосуванням інформаційних технологій, їхня армія здатна належним чином відповісти супротивнику, адже принцип максимального використання внутрішніх сил у протидії зовнішнім — у національних традиціях Китаю. За рівнем інформаційних технологій і інформаційної зброї Китай у майбутній війні навряд чи зможе перевершити потенційного супротивника, тому його стратегічна лінія буде спрямована на активну оборону своїх рубежів з максимальним залученням внутрішніх ресурсів. У контексті інформаційної війни це означає посилення заходів щодо маскування своїх військ, підвищення активності протиповітряної оборони, атаки і перехоплення бойових засобів, що застосовують високоточну зброю, у момент, коли супротивник цього не очікує і т. д.

Китайські військові аналітики припускають, що успішне ведення інформаційної війни зажадає від збройних сил повного використання переваг території країни і засобів розвідки з метою раннього виявлення намірів супротивника, його підготовки до наступальних дій; розробки, удосконалення і застосування наявних на озброєнні ефективних інформаційних технологій; посилення акценту на веденні мобільних бойових дій; організації операцій по деморалізації військ ворога; формування спеціальних сил ведення інформаційної війни, їхнього оснащення сучасною зброєю, розробленою на базі нових ІТ. Вони упевнені, що розвиток інформаційних технологій неминуче викликає революцію у військовій справі, і ця революція вже розпочалася. Той, хто першим візьме у ній участь, виявиться на хвилі прогресу розвитку людського суспільства. Зазначена революція — це насамперед *революція концепцій*, а потім уже прогрес у науці і техніці, стратегії і тактиці, навчанні військовій справі. Тому найважливішою проблемою, що вимагає ретельного пророблення, є підготовка і ведення інформаційної війни.

1.3.2.2. Значення психологічних операцій в інформаційній війні

Пропагандистське розкладання військ і населення супротивника має настільки ж давню історію, як і воєнне мистецтво. Протиборствуючі сторони і сотні, тисячі років тому знали, що

боротися з ворогом можна не тільки за допомогою зброї, а і шляхом цілеспрямованого психологічного впливу, намагалися використовувати засоби духовного впливу для ослаблення морального духу і бойової могутності ворога.

Уже приблизно в V столітті до н.е. китайський полководець, військовий теоретик і філософ Сунь Цзи у своєму трактаті «Мистецтво війни» писав, що «найкраща політика полягає в захопленні держави цілісною, зруйнувати її значно легше. Взяти в полон армію супротивника краще, ніж її знищити. Одержати сотню перемог у сотні боїв — це ще не межа мистецтва. Покорити супротивника без бою — от вінець мистецтва».

У цій широко відомій праці підкреслюється, що найвигідніша з усіх військових стратегій — маніпулювання ворогом у такий спосіб, щоб домогтися легкої перемоги над ним без бою. Сунь Цзи першим узагальнив досвід, накопичений стародавнім Китаєм у сфері психологічних операцій. Він стверджував, що найгірше — напад на ворожі укріплені міста. У Китайській Народній Республіці цю концепцію перефразували так: «Краще атакувати розум супротивника, аніж його укріплені міста».

Теоретичні побудови основоположника психологічної війни закликають: «Розкладайте все хороше, що є в стані вашого супротивника; втягуйте його відомих представників у злочинні заходи, підривайте їхній престиж, виставляйте їх у потрібний момент на ганьбу громадськості; використовуйте співробітництво найбільш підлих і мерзенних людей; розпалюйте сварки і зіткнення серед громадян ворожої країни; перешкоджайте всіма способами оснащенню, забезпеченню і наведенню порядку в збройних силах ворога; будьте щедрі на пропозиції і подарунки для купівлі інформації і підкупу спільників; не економте ні на грошах, ні на обіцянках, тому що вони приносять багаті дивіденди».

Подальший розвиток воєнного мистецтва незмінно супроводжувався удосконаленням форм морального впливу на супротивника. До II століття н.е. відносять появу самостійної теми пропаганди — проголошення справедливого чи несправедливого характеру війни. Ні чим іншим, як прагненням підірвати бойовий дух воїнів ворога можна пояснити звичай, коли одна з воюючих сторін виступає з тим чи іншим обвинуваченням на адресу свого суперника і закликає своїх союзників і однодумців у кон-

фронтуючому стані приєднатись до «боротьби за праведну справу». Цей прийом широко використовувався правителями Стародавнього Китаю досить тривалий час. Пред'явлене до початку чи на самому початку збройного зіткнення обвинувачення слугувало в ході всієї війни надійним обґрунтуванням законності дій, спрямованих на знищення ворога.

Здавна в Китаї вважали одним із найбільш надійних засобів для цього обман (дезінформацію) — пряме маніпулювання поглядами супротивника на реальність з метою спонукати його вживати заходів у бажаному напрямі. Знову звернемося до Сунь Цзи. Він писав: «Війна — гра обману. Тому прикидайся немичем, коли сильний; прикидайся млявим, коли готовий завдати удару; здавайся далеким, коли насправді знаходишся поруч, і навпаки. Коли ворог жадає наживи, підмани його наживкою; коли він у безладді, напади і здобудь перемогу над ним; коли він хвалиться значними силами, будь подвійно готовий діяти проти нього; коли він страшний, обходь його. Якщо він податливий до гніву, провокуй його. Якщо він боязкий і обережний, заохочуй його марнославство. Якщо сили його свіжі, вимотай їх. Якщо він єдиний, розділи його. Атакуй його, коли він найменше готовий. Дій, коли він найменше тебе очікує. У цьому полягають тонкощі командування стратега, що неможливо заздалегідь передати чітко визначеними правилами, готовими для негайного застосування».

Недавнє минуле засвідчило, що керівництво Компартії Китаю, командування створених нею збройних сил (Народно-визвольна армія Китаю — НВАК) непогано засвоїли уроки свого мудрого співвітчизника.

Під час громадянської війни вони успішно вели психологічні операції, добре знаючи своїх супротивників, їхні сильні і слабкі сторони, використовуючи наявні можливості для контролю за потоками інформації. КПК і НВАК, зокрема, намагалися переконати воюючих проти них гоміньданівців, що їхні вороги дурні, боягузливі, слабкі, відступатимуть при першому ж натиску. Крім того, особливий наголос робився на складному поєднанні пропаганди і чуток, щоб спонукати лідерів націоналістів роздрібнити армію і направити її з'єднання аж ніяк не туди, куди варто було б.

Після утворення КНР (1949 рік) у всіх конфліктах, у яких брала участь НВАК, психологічні операції були обов'язковою складовою її стратегії. Так, під час Корейської війни (1950 — 1953 роки) політичні органи НВАК постійно прагнули за допомогою агітаційно-пропагандистських матеріалів подати її як агресію американського імперіалізму, дискредитувати військово-політичне керівництво США і Південної Кореї, вихвалити бойову міць і військові успіхи північнокорейських і китайських військ, демонструвати випадки расової дискримінації в армії США.

Особливу увагу китайські підрозділи спецпропаганди приділяли закликам здаватися в полон. Аргументи, що наводилися в розповсюджуваних ними листівках, мали посіяти страх у солдатів супротивника перед невизначеністю того, що їх чекає «на тому боці», підводили до думки про те, що доцільно перебігти до ворога в ім'я кінцевої мети — повернутися додому живим. Причому багато матеріалів копіювали композиційні і стилістичні особливості американських газет, нерідко повідомлення підтверджувалися посиланнями на назви друкованих ЗМІ США з указівкою дати їхнього випуску. Листівки, так би мовити, «сентиментального характеру» були покликані викликати тугу за батьківщиною, занепокоєння за власне життя. Серед них виділялася серія різдвяних листівок-поздоровлень, виконаних у стилі традиційних американських листівок з написаним на звороті побажанням щастя в новому році.

Китай також продемонстрував, що він здатний успішно вести «чорну пропаганду». Яскравим прикладом цього є зчинений під час Корейської війни галас про застосування США біологічної зброї, щоб викликати стосовно КНР і КНДР симпатії міжнародної громадськості.

Водночас відносна ізольованість Китаю від Заходу до початку 1970-х років залишала мало місця для використання дезінформації в повсякденних міждержавних відносинах. У ході психологічної війни проти Москви і Вашингтона в 1960 — 70-х роках вихвалялась, головним чином, стратегія стримування, щоб змінити поведінку своїх опонентів на довгострокову перспективу. Пропаганда цього періоду була одним із основних елементів національної стратегії, результатом якої стало прийняття в 1972 році КНР в ООН і встановлення дипломатичних відносин між Пекіном і Вашингтоном.

Аналіз воєнної доктрини КНР і її сучасних положень дає змогу визначити ряд завдань, що їх мають вирішувати політичні органи НВАК у сучасній війні. На початковому етапі пропаганда буде спрямована на ослаблення морального духу і дискредитацію тимчасових успіхів супротивника. Після відбиття стратегічного наступу ворога необхідно, використовуючи успіхи оборонних боїв, усіляко його деморалізувати, посіяти в нього сумніви в можливості досягнення поставлених у війні цілей, схилити певну частину його солдатів і офіцерів до переходу на свій бік. Коли потім розгорнеться стратегічний контрнаступ, підуть заклики до масової здачі в полон військовослужбовців супротивника, особливо тих, які потрапили в оточення. При перенесенні бойових дій на чужу територію до завдань політorganів належатиме також морально-психологічна обробка населення окупованих НВАК районів.

Китайські військові аналітики вважають, що сьогодні нездатність протистояти іноземному інформаційно-психологічному втручання є небезпечнішою, ніж відсталість у інших галузях. Розвиток технологій у наші дні, на їхню думку, дав можливість активно впливати на всіх людей — від рядових громадян до глав держав. Імітація промов, нібито виголошених лідерами країн, фальсифікація фото- і кіноматеріалів з наступною демонстрацією невідповідної аудиторії — усе це може серйозно вплинути на населення і військовослужбовців протиборствующої сторони.

Можна сміливо стверджувати, що тактика і стратегія ведення психологічної війни активно розробляється провідними військовими теоретиками НВАК. Деякі роботи з цієї тематики дають підстави говорити про наявність у них свого роду «китайської специфіки». По-перше, привертає до себе увагу широке використання історичного матеріалу й основних принципів китайського воєнного мистецтва, що має тисячолітні традиції. Цьому робиться наголос на проведенні психологічних операцій у мирних умовах, вони розглядаються як підготовчий етап повномасштабної інформаційної війни в умовах відкритого збройного протистояння.

Інтенсифікація розробок по організації і веденню подібних операцій дає всі підстави вважати, що незабаром вони набудуть у КНР найбільшого поширення⁴⁴.

1.3.3. Погляди фахівців Російської Федерації на проблеми інформаційного протиборства

1.3.3.1. Погляди фахівців Російської Федерації на місце і роль інформаційної боротьби в забезпеченні національних інтересів

Проблемам інформаційної безпеки, зокрема інформаційної боротьби, особливу увагу останнім часом приділяють у Росії, про що свідчать наукові публікації фундаментального характеру в її провідних науково-технічних періодичних виданнях. Доречно зазначити, що генерал О. Лебедь після призначення на посаду секретаря Ради національної безпеки Російської Федерації серед п'яти пріоритетних напрямів розвитку Збройних Сил Росії назвав інформаційну боротьбу.

Показовим є Перелік основних напрямів фундаментальних досліджень у галузі оборонної безпеки, запропонований Академією військових наук Російської Федерації⁴⁵. Для повного уявлення про те, яке значення приділяється фахівцями РФ інформаційній компоненті в забезпеченні воєнної безпеки держави та інформаційній боротьбі, доречно навести ті напрями досліджень з цього переліку, які безпосередньо стосуються інформаційної боротьби (номери розділів і пунктів наводяться відповідно до Переліку).

«Розділ I. Загальні основи наук про війну і оборонну безпеку:

16. Проблеми зовнішньої розвідки і контррозвідки в мінливому світі.

Розділ II. Військова наука і оборонна проблематика гуманітарних, природничих наук:

Теорія стратегії:

1. Тенденції розвитку теорії стратегії за нової розстановки сил у світі, зміненому характері воєнних загроз і зростаючому значенні інформаційної боротьби.

3. Види війн і збройних конфліктів, способи їх запобігання і нейтралізації шляхом узгоджених політико-дипломатичних, інформаційних і воєнно-стратегічних акцій.

II. Організація і способи ведення інформаційної боротьби і інформаційних операцій у стратегічному масштабі.

12. Шляхи вдосконалення управління збройними силами в їх новій (тривидовій) організаційній структурі з використанням нових інформаційних технологій і засобів автоматизації.

Теорія оперативного мистецтва:

7. Шляхи удосконалення оперативного забезпечення сучасних операцій (інформаційної боротьби, розвідки, інженерного забезпечення, оперативного маскування, РЕВ, захисту від ЗМУ та ін.).

11. Управління військами (силами) за значної насиченості управлінської діяльності інформаційними процесами і напруженого радіоелектронного протиборства.

21. Проблеми удосконалення організації і способів виконання завдань органами і частинами ФАУЗІ (Федерального агентства урядового зв'язку та інформації) в умовах загострення інформаційної боротьби.

Теорія тактики:

7. Управління військами (силами) в умовах жорсткої інформаційної і радіоелектронної протидії.

Теорія озброєнь:

5. Концепція державної програми першочергового розвитку засобів зв'язку, навігації, розвідки, наведення, космічних засобів, автоматизованих засобів управління і радіоелектроніки.

Оборонні галузі (воєнна проблематика) гуманітарних (суспільних), природничих і технічних наук:

2. Інтеграція зусиль ряду галузей суспільних, природничих і технічних наук для досліджень і розробки проблем інформаційної боротьби.

Розділ III. Галузі наук, що досліджують невоєнні форми забезпечення оборонної безпеки».

У науковому плані невоєнні форми забезпечення оборонної безпеки досліджуються галузями наук, пов'язаними з політико-дипломатичною діяльністю, соціально-політичною, економічною, екологічною, інформаційною, технологічною, духовною та іншими сферами національної безпеки.

Із них найбільш пріоритетними є дослідження і розробка шляхів розв'язання політичних, економічних та інших суперечностей невоєнними засобами, використання військової сили для підкріплення політико-дипломатичних і економічних акцій.

1.3.3.2. *Форми і методи забезпечення оборони країни і протидії міжнародним силам та іншим країнам в інформаційній боротьбі*

Цікавим є коментар російського фахівця стосовно сформульованих напрямів досліджень академії військових наук РФ: «Вченими Академії військових наук розроблена нова класифікація воєнних знань, яка відбиває зміни геополітичної і воєнно-політичної обстановки, а також результати розвитку науки і техніки.

Вчені дійшли висновку, що в нашій країні не вироблено потрібних заходів і рішень щодо протидії політико-дипломатичним, економічним, інформаційним та іншим невоєнним методам впливу на Росію, ущемлення її інтересів, підризу держави зсередини.

Одним з найважливіших результатів діяльності академії є розробка проблем стратегії непрямих дій, пошук нових засобів впливу на противника, включаючи інформаційні, психологічні, спеціальні операції.

Нарешті, вчені академії зосередяться на дослідженні проблем інформаційної боротьби»⁴⁶.

Підтвердженням того, якого значення надають російські фахівці інформаційним засобам протиборства, є стаття іншого російського дослідника цих проблем⁴⁷. Розробка і вдосконалення нетрадиційних засобів протиборства в рамках сучасного етапу воєнно-технічної революції привели до створення нового класу озброєння — зброї глобального ураження (ЗГУ), тобто зброї, системне застосування якої здатне забезпечити глобальний характер ураження середовища проживання людини (СПЛ). До неї належать інформаційна, нелегальна і екологічна зброя.

Якщо розглядати інформаційну зброю як сукупність засобів, що застосовуються для порушення (копіювання, спотворення чи знищення) інформаційних ресурсів на стадіях їх створення, обробки, розповсюдження і (або) зберігання, то в структурі інфосфери слід виділити такі основні об'єкти її впливу, як:

- програмне та інформаційне забезпечення;

- програмно-апаратні, телекомунікаційні та інші засоби обробки інформації та управління;

- канали зв'язку, що забезпечують циркуляцію інформаційних потоків і інтеграцію систем управління;

- інтелект людини і масова свідомість.

Відомо, що інформаційні засоби протиборства на сучасному етапі розвиваються найбільш динамічно. Напевне, це пояснюється такими якостями інфосфери, як невичерпність і відновлення інфоресурсів, можливість їх швидкого копіювання з високим ступенем достовірності, а також можливість переміщення великих обсягів цих ресурсів практично без втрат, з високою швидкістю і на величезні відстані, компактність джерел і носіїв інформації, миттєва, але безкровна реакція (відгук) інфосфери на важко ідентифікований (щодо джерел) вплив та ін.

1.3.3.3. *Погляди російських військових фахівців на роль інформаційної компоненти у війнах майбутнього*

Особливості бойового застосування високоточної зброї зумовили необхідність інтеграції різних засобів збройної боротьби в єдині системи високоточної зброї — розвідувально-ударні комплекси. Ці комплекси являтимуть собою складні системи функціонально взаємопов'язаних засобів розвідки, управління, забезпечення і поразки. Складність таких систем не стане перешкодою для їхнього використання в умовах війни. Вони будуть цілком надійними, стійкими до радіоелектронної протидії і не потребуватимуть особливої підготовки обслуговуючих їх операторів.

Існуючі й розроблювані у провідних країнах світу високоточні крилаті та інші ракети звичайного типу наземного, повітряного і морського базування можуть застосовуватися лише в умовах інформаційної переваги. Буде потрібно за допомогою засобів інформатики, розвідки і зв'язку швидко одержати точну, своєчасну і захищену інформацію, що дасть змогу правильно реагувати на будь-який конфлікт із метою негайного оволодіння ситуацією і прийняття необхідних рішень. Для цього, очевидно, доведеться розробити зовсім інші, ніж нині, глобальні військові системи командування, управління, розвідки і зв'язку. Виникне потреба мати комунікацію інформаційних мереж, що перекриватимуть усі сфери збройної боротьби практично по всій земній кулі. Одночасно буде потрібно перешкоджати супротивнику в одержанні інформації для управління його

військами і зброєю. Інформаційна перевага має бути реалізована через перевагу в мобільності, у швидкості реакції, у точному впливі на супротивника й у мінімально можливому ризику для своїх сил і засобів. Інформаційна перевага має бути реалізована: шляхом панування в маневрі силами, засобами і вогнем; масового і тривалого за часом застосування високоточної зброї, адресного всебічного матеріально-технічного забезпечення; надійного захисту сил і засобів на всіх рівнях.

Інформаційна складова найбільш високоточної зброї, на думку заслуженого діяча науки Російської Федерації, академіка Академії військових наук, доктора військових наук, професора, генерал-майора В. Сліпченка, матиме повний набір програмних засобів і заходів як активного і пасивного захисту від атак на його інформаційні системи, так і впливу щодо всіх існуючих і перспективних систем ППО і ПРО супротивника і діятиме разом з космічними засобами розвідки цілей і об'єднаною радіолокаційною системою виявлення і наведення. Засоби розвідки також набудуть значного розвитку, тому що на них будуть покладені завдання пошуку, виявлення, ідентифікації і виміру необхідних параметрів стаціонарних об'єктів економіки, що мають бути знищені високоточними крилатими чи міжконтинентальними ракетами. Використовуватимуться командні пункти космічного і повітряного базування для спрямування ударів по найважливіших стаціонарних і рухливих цілях.

Для виявлення наземних цілей, що підлягають знищенню в глибині території супротивника, очевидно, буде потрібно створити дешевші ніж космічні, але високоефективні безпілотні літакові засоби стратегічної розвідки. Розвідувальний потенціал держав може істотно підвищитися саме за рахунок безпілотних літальних апаратів з великою тривалістю польоту.

Слід зазначити, що в ряді найбільш розвинутих країн у різних видах їхніх збройних сил, родах військ уже сьогодні мається велика кількість різнотипних сил і засобів розвідки, однак усі вони значною мірою роз'єднані. У війнах і воєнних конфліктах майбутнього буде необхідною висока інтеграція численних розвідувальних систем для їхнього автоматизованого розподілу в глобальній інформаційній мережі по всій земній кулі. Виникне необхідність серйозного об'єднання систем розвідки космічного

і повітряного базування. Є неминучим підвищення гнучкості застосування й універсальності засобів розвідки.

У повітряно-космічних силах і засобах розвідки у майбутніх війнах переважатимуть безпілотні літальні апарати, кількість яких на рубежі 2000 року в західних країнах сягне 30 тис. Один з подібних літаків уже був продемонстрований у США в середині лютого 1997 року в Сан-Дієго (штат Каліфорнія). Цей літак має розрахункову дальність польоту до 25 тис. км і може перебувати в повітрі протягом 42 годин на висоті 22 км. На борту безпілотного літака містяться оптичні й інфрачервоні телекамери, радіолокаційна станція, а також станції радіо- і радіотехнічної розвідки. Бортова апаратура дає змогу робити детальну зйомку місцевості з точністю до 30 див і безупинно передавати розвіддані по супутникових каналах зв'язку безпосередньо на центральний командний пункт Збройних сил США. Є відомості, що інший літак-розвідник подібного типу також розробляється в США. Правда, його характеристики дещо нижчі — тривалість польоту 12 годин на висоті 15 тис. км. Однак цей літак розробляється за програмою «Стеле», тобто він буде невидимкою для засобів виявлення. США мають намір мати до початку нового століття і тисячоліття 120 — 150 стратегічних літаків-розвідників, а надалі їх кількість може сягати 500 — 600 одиниць. Не виключена можливість, що частина таких літаків буде виготовлена і для інших країн — Великої Британії, Франції, Німеччини, Китаю, Тайваню.

У цей перехідний період діятимуть спільно стратегічні ядерні засоби, повітряні, морські й сухопутні сили, засоби доставки високоточної зброї і зброї на нових фізичних принципах. Значною мірою цьому сприятиме також триваюча розробка, крім високоточних засобів і інших типів озброєнь, передусім зброї, спрямованої передачі енергії, автоматичних і автоматизованих систем наведення високоточної зброї, нових вибухових речовин підвищеної могутності, засобів обробки даних надвисокої швидкодії, а також засобів радіоелектронної боротьби.

Після завершення перехідного періоду у війнах шостого покоління широко застосовуватимуться засоби поразки, дія яких по об'єктах (цілях) ґрунтуватиметься на використанні фізичних форм енергії, а також відповідних засобів захисту від їхнього впливу. Можна стверджувати, що й у збройній боротьбі май-

бутнього головною залишиться фізична боротьба. Однак зовсім не виключена можливість, що в цій боротьбі застосовуватимуться й інші засоби поразки.

В арсеналах деяких, головним чином, відсталих країн у перехідний період залишиться на озброєнні хімічна зброя (ядерна зброя бідних), яку вони цілком ймовірно можуть застосувати, не побоюючись за наслідки. У разі застосування таких засобів поразки буде потрібно мати і застосовувати відповідні засоби захисту від їхнього впливу. Такий вид збройної боротьби належатиме до хімічної боротьби. Здається, що після закінчення перехідного періоду буде вжито всіх заходів, спрямованих на повну ліквідацію цієї зброї на нашій планеті.

Ймовірно, в перехідний період може набути розвитку і біологічна зброя. Вона також може бути на озброєнні ряду економічно відсталих, але екстремістських країн. Вид збройної боротьби, в якому поразка завдаватиметься шляхом біологічного впливу і застосовуватимуть відповідні засоби захисту, можна назвати біологічною боротьбою. Є підстави вважати, що за допомогою ООН, Ради Безпеки ця зброя буде поставлена поза законом і у разі її розробки до таких країн будуть застосовані усі можливі, в тому числі силові, заходи для припинення виробництва і ліквідації наявних запасів.

У війні і збройній боротьбі майбутнього для виведення з ладу обслуговуючого персоналу об'єктів економіки може мати застосування і зброя на нових фізичних принципах (НФП) — акустична поразка. Вона може доставлятися у великих кількостях за допомогою високоточних крилатих і балістичних ракет, викидатися на парашутах, скидатися на землю в районі об'єктів і проникати усередину об'єктів, що підлягають знищенню. У цьому виді вражаючого впливу використовуватиметься енергія акустичних випромінювань певної частоти й енергія, яка генерується акустичною зброєю. Така поразка може викликати деморалізацію і навіть загибель усього живого, порушувати роботу чи виводити з ладу ті радіоелектронні засоби, що працюють на принципі прийому і перетворення акустичних хвиль, руйнувати окремі елементи деяких видів зброї, військової техніки й об'єктів. Носіями такої зброї можуть бути наземні, морські, повітряні й космічні засоби.

Значного розвитку набуде зброя НФП електромагнітного ураження. Вона являтиме собою вид вражаючого впливу на об'єкти, цілі з використанням енергії електромагнітних випромінювань різних довжин хвиль і рівнів потужностей, генерованих радіочастотною і лазерною зброєю, засобами радіоелектронної протидії (РЕП) чи висотними ядерними вибухами. Така зброя буде здатна придушувати практично всі класичні радіоелектронні засоби (РЕЗ), що працюють на принципі прийому і перетворення електромагнітних хвиль; викликати розплавлення чи випаровування металу зброї і військової техніки або викликати структурні зміни електронних елементів військової техніки; впливати на поведінку людини; руйнувати живі клітини, порушувати біологічні й фізіологічні процеси у функціях живих організмів. Носіями такої зброї можуть бути ракетні системи наземного, морського і повітряного базування, застосовувані по настільних траєкторіях, безпілотні засоби великої дальності дії.

Ефективне ураження і захист у війнах і збройній боротьбі майбутнього зумовлять необхідність кардинального розвитку засобів розвідки. Розвідка в збройній боротьбі майбутнього також змінить свій статус і стане невід'ємним елементом і змістом будь-якого удару, бою, операції, а не їх забезпеченням, як прийнято в даний час. Єдність розвідки і поразки як одна з головних ознак збройної боротьби майбутнього особливо наочно помітні на прикладах функціонування розвідувально-ударних бойових систем (РУБС) і розвідувально-вогневих комплексів (РВК).

Аналогічні міркування застосовні і до визначення місця маскування у війнах і збройній боротьбі майбутнього. Засоби і прийоми маскування, застосовувані узгоджено з діями великої кількості високоточних засобів і зброї на нових фізичних принципах у поєднанні з поразкою засобів розвідки, вводитимуть в оману супротивника і, незважаючи на те, що вони безпосередньо не уражають цілей, знижуватимуть чи навіть виключатимуть його можливості щодо радіоелектронного придушення і вогневої поразки військ і об'єктів. Тому в збройній боротьбі майбутнього маскування також цілком очевидно вилучать з видів забезпечення на всіх рівнях і віднесуть до змісту бойових дій, зокрема до заходів щодо захисту військ від поразки.

Що стосується поняття «забезпечення бойових дій», то у війнах і збройній боротьбі майбутнього до нього будуть віднесені тільки ті специфічні заходи, що створюють умови для дій, спрямованих на ураження супротивника чи захист від нього. Тут поняття «забезпечення» повною мірою відповідатиме його змісту: постачання всім необхідним, недопущення нестачі чого-небудь і т. п. Відтак, забезпеченням бойових дій у збройній боротьбі майбутнього можна буде вважати лише тиловий і технічний їх види.

При цьому зросте значення радіоелектронної боротьби (РЕБ). З виду забезпечення бойових дій у війнах четвертого покоління вона перетвориться на новий самостійний рід військ і здійснюватиме свою форму оперативно — стратегічних дій — операцію РЕБ. За своїми цілями, завданнями, силами і засобами ця операція дуже тісно переплітатиметься і повною мірою узгоджуватиметься в усіх напрямках як з діями стратегічних ударних, так і стратегічних оборонних сил і засобів.

Під операцією РЕБ у збройній боротьбі майбутнього маєт-ся на увазі комплекс заходів і дій по радіоелектронному придушенню супротивника і захисту своїх військ (сил) і систем озброєння від радіоелектронного придушення. Складовими частинами операції РЕБ будуть: радіоелектронні удари з метою придушення всієї системи радіоелектронних засобів супротивника; радіоелектронна оборона (захист) об'єктів і засобів; заходи щодо забезпечення операції РЕБ.

Радіоелектронні удари (РЕУ) являтимуть собою заходи і дії, здійснювані військами (силами) по прицільному і загальному придушенню та дезінформуванню всієї системи радіоелектронних засобів супротивника енергією електромагнітних (акустичних) випромінювань. У збройній боротьбі майбутнього для гнітючого впливу на РЕЗ супротивника разом із засобами РЕП широко застосовуватимуться і різні засоби вогневої поразки, головним чином високоточних міжконтинентальних і крилатих ракет великої дальності дії, самонавідні на джерела електромагнітного (акустичного) випромінювання.

Дезінформація в операції РЕБ також застосовуватиметься для введення супротивника в оману шляхом удаваної роботи РЕЗ своїх військ (сил), зміни режимів і характеристик їхньої роботи й імітації роботи РЕЗ супротивника. Основними способами дез-

інформації залишатимуться: керована демонстрація помилкових демаскуючих ознак РЕЗ, об'єктів і обстановки; навмисне кваліфіковане входження в радіомережі і радіонапрями супротивника, передача в них хибної інформації і команд, перекручування відомостей, сигналів і позивних; посилення (імітація) інтенсивності роботи РЕЗ на другорядних і удаваних напрямках за збереження режиму роботи на головному. Слід зазначити, що дезінформація в операції РЕБ матиме успіх тільки в разі одночасного і комплексного застосування засобів, що імітують наявність і рух цілей, а також засобів, що маскують передані сигнали для введення в оману РЕЗ супротивника. Радіодезінформування здійснюватиметься в поєднанні і з такими заходами, як агентурні дані, поширення чуток, фізична імітація перекидання сил і засобів, реальне завантаження дорожньої мережі, підвезення чи вивезення вантажів, спорудження відволікаючих об'єктів, демонстрація заняття ударними засобами вихідного положення, відповідні активність і перегрупування авіації тощо.

Радіоелектронна оборона (захист) (РЕО) в операції РЕБ являтиме собою комплекс заходів щодо радіоелектронного прикриття об'єктів, що обороняються, об'єктів економіки, ударних і оборонних військ та засобів, а також забезпечення ефективного і стійкого функціонування своєї системи РЕЗ в умовах впливу на них засобів РЕП супротивника. Вона досягатиметься приховуванням РЕЗ і промислових об'єктів від радіоелектронної розвідки (РЕР) і захистом від їхнього радіоелектронного придушення, а також контролем за випромінюванням РЕЗ своїх військ (сил) і систем зброї.

Заходи щодо забезпечення операції РЕБ (радіоелектронне забезпечення операції) включатимуть пошук, перехоплення й аналіз випромінювань, впізнання і визначення місця розташування РЕЗ і систем супротивника, оцінку створюваної ними загрози для нанесення по них наступних радіоелектронних ударів (придушення) чи видачі цілевказівки засобам поразки, а також управління своїми силами і засобами РЕП.

Дії, проведені в ході операції РЕБ, у поєднанні з вогнем і маневром також здійснюватимуться відповідно до обстановки, що складається, одночасно: або з повітряно-космічною наступальною операцією; або зі стратегічною операцією по відбиттю повітряно-космічного нападу супротивника. У зв'язку з різким

збільшенням масштабів застосування високоточних засобів поразки в збройній боротьбі майбутнього можливості і роль РЕУ і РЕО значно зростають. Необхідно буде здійснювати безупинне перехоплення, аналіз електромагнітних і акустичних випромінювань і радіопеленгування їхніх джерел за допомогою наземних, повітряних надводних і космічних розвідувальних систем.

Якщо стратегічними ударними силами здійснюється повітряно-космічна наступальна операція, то операція РЕБ починатиметься за кілька годин до злету ракетonoсної авіації радіоелектронними ударами з метою придушення радіоперешкодами каналів державного і військового керівництва супротивника, потім міць ударів нарощуватиметься засобами перешкод численних груп літаків РЕБ, що діють із зон баражування без перетинання кордонів супротивника, по придушенню об'єктів систем раннього радіолокаційного попередження, наведення винищувальної авіації й управління військами. Ешелон прориву системи ППО — ПРО, що повністю складається з безпілотних високоточних засобів, у ході повітряно-космічної наступальної операції забезпечуватиме (прикриватиме), не перетинаючи кордону, літаки РЕБ, що, крім ефективного радіоелектронного придушення всіх радіоелектронних засобів противника, будуть здатні уражати найважливіші з них протирадіолокаційними ракетами.

Протягом усієї операції РЕБ спостерігатиметься винятково висока спектральна щільність потужності випромінюваних прицільних і загороджувальних перешкод (декілька тисяч Вт/Мгц), створюваних угрупованням РЕБ на землі, у повітрі й у космосі, що унеможливить використання супротивником радіолокаційних станцій (РЛС), засобів зв'язку та інших радіоелектронних засобів і систем практично в усіх частотних діапазонах.

Особлива роль у збройній боротьбі майбутнього відводиться *інформаційному ресурсу*. Високоточна зброя і зброя на нових фізичних принципах, на які будуть покладені завдання, що завжди вирішували здебільшого лише великі угруповання живої сили, зажадає мати необхідну розвідувальну інформацію. Виникне гостра потреба в різних інформаційних комплексах, реалізованих у засобах розвідки й управління, а також у силах і засобах РЕБ. Для ведення розвідки широко застосовуватимуться космічні, морські і наземні сили та засоби розвідки.

Виникне потреба безупинно і детально спостерігати за всією територією супротивника, за станом його стратегічних ударних і стратегічних оборонних сил, за всіма переміщеннями його військ (сил) у межах театру воєнних дій.

Космічні засоби розвідки стануть основним джерелом інформації як при плануванні, так і при організації і веденні бойових дій. З космічного простору постійно і широко здійснюватиметься радіотехнічна, радіолокаційна, фото-, телевізійна, інфрачервона, радіаційна, хімічна розвідка, які безупинно видаватимуть необхідну інформацію в реальному масштабі часу. У війні в зоні Перської затоки, наприклад, широко використовувалися американські розвідувальні супутники «Лакрос», що передавали з космосу радіолокаційне зображення району бойових дій. Їхнє використання дало можливість оцінювати ефективність високоточних і повітряних ударів, розкривати з достатньою мірою точності оборону іракської армії до окремої бойової машини чи зенітної артилерійської гармати навіть в умовах поганої видимості. Слід очікувати, що ще до 2000 року орбітальні угруповання подібних розвідувальних космічних апаратів ряду держав будуть значно посилені. У найближчі 10 — 15 років мають різко зрости можливості космічних засобів розвідки найбільш розвинутих країн: за кількістю об'єктів, що розкриваються, вони збільшаться в три — чотири рази, за точністю виявлення підвищаться в чотири — шість разів, а час на розвідку при цьому зменшиться в три — чотири рази.

Космос продовжуватиме мати велике воєнне значення не тільки як сфера забезпечення воєнних дій на землі, а й як театр воєнних дій, де може застосовуватися зброя неядерного типу, в тому числі й щодо об'єктів і цілей на наземних театрах воєнних дій.

Управління військами (якщо вони деякою мірою збережуться в нинішньому розумінні), силами і засобами здійснюватиметься головним чином з командних пунктів, піднятих у космос і повітря, чи з захищених командних пунктів на землі, але через повітряно-космічні засоби. Значно збільшиться кількість літаків управління і далекого радіолокаційного виявлення. Інформаційний обмін здійснюватиметься між усіма ланками і рівнями командування за допомогою автоматичних чи автоматизованих систем, розміщених на повітряних і космічних засобах.

У збройній боротьбі майбутнього, як зазначалося, широко застосовуватимуться розвідувально-ударні бойові системи (РУБС) на базі космічних розвідувально-інформаційних систем, а також наземних, морських, повітряних і космічних високоточних засобів поразки. Вони завдаватимуть ефективних ударів по стаціонарних радіо- і тепловипромінюючих промислових об'єктах, засобах повітряно-космічної оборони, а також по радіолокаційно-контрастних цілях на всю глибину території супротивника. Слід підкреслити, що частина таких РУБС космічного базування може бути створена заздалегідь, ще в мирний час, і вони можуть бути націлені на найважливіші стаціонарні цивільні та військові об'єкти ймовірних супротивників.

Зрозуміло, для підготовки і ведення збройної боротьби майбутнього державі буде потрібно перейти від індустріального до інформаційного суспільства, мати можливість здійснювати космічне навігаційне забезпечення кожного високоточного засобу поразки. Стає цілком очевидним, що одним з атрибутів війни майбутнього стане «інформаційне протиборство». Правда, деякі фахівці намагаються довести, що вестиметься не «інформаційне протиборство», а «інформаційна війна». Однак поняття «війна» в даному разі не підходить, тому що це складне суспільно-політичне явище. Вона являє собою протиборство суспільних систем, класів, націй, держав із застосуванням збройного насильства для досягнення політичних цілей. Здається, що не слід очікувати єдиного і чіткого визначення поняття «інформаційна війна». «Інформаційне протиборство» чи «інформаційна боротьба» є цілком законними термінами і виражають боротьбу сторін за перевагу в кількості, якості й швидкості добування, аналізу та застосування інформації. Зрозуміло, що цей вид протиборства також, як і інші його види, має дві складові — оборонну і наступальну, або ударну. Оборонна — має захистити свою інформацію від впливу супротивника. Ударна — дезорганізувати чи зруйнувати інформаційну інфраструктуру супротивника, порушити процес оперативного управління його силами і засобами. Очевидно, на позначення ударної складової інформаційного протиборства можна використовувати і поняття «інформаційна інтервенція» чи «інформаційна агресія». Оскільки вже чітко окреслилось прямування у бік воєн нового покоління,

роль інформаційного протиборства різко зростає в таких напрямках, як: боротьба з системами управління; нав'язування супротивнику своїх правил ведення воєнних дій; ставка на військово-технічну перевагу. Інформаційне протиборство набуло могутнього розвитку після створення сучасних методів воєнної системології. Використовуючи ці методи, можна швидко знайти уразливі місця системи керування, зв'язку, комп'ютерного забезпечення і розвідки супротивника і, виводячи їх з ладу, значно підвищити ефективність своїх дій у інших видах протиборства. Критичними ланками системи управління супротивника є інформаційні засоби, руйнування або знищення яких веде до негайного зниження його можливостей по управлінню військами і силами. Вершиною інформаційного протиборства, очевидно, стане створення *глобальної бойової інформаційно-ударної системи країни і збройних сил*, здатної контролювати стан і функціонування збройних сил і угруповань супротивника та знижувати ефективність їхнього застосування.

Прояв великого інтересу до інформаційного протиборства не випадковий, тому що це пов'язано з тим, що інформація стає такою самою зброєю, як і ракети, бомби, торпеди і т.п. Уже нині зрозуміло, що інформаційне протиборство є тим фактором, що впливає на саму війну майбутнього.

Отже, під інформаційним протиборством слід розуміти нову форму боротьби сторін, у якій використовуються спеціальні способи і засоби, що впливають на інформаційне середовище супротивника і захищають в інтересах досягнення стратегічних цілей війни. Однак інформаційне протиборство ніколи не припинялося, воно відбувається і зараз, тому що сторони завжди прагнули контролювати інформацію супротивника не тільки у воєнний, а й у мирний час. Володіння інформаційними ресурсами у війнах майбутнього стає таким самим неодмінним атрибутом, як у минулих війнах розгром збройних сил супротивника, оволодіння його територією, руйнування його економічного потенціалу і повалення політичного режиму. Цілі і завдання інформаційного протиборства є основою побудови його змісту, а отже, і структури його наукової теорії.

У найзагальнішому вигляді головною метою інформаційного протиборства (інформаційної боротьби), як зазначалося, є збе-

реження необхідного рівня своєї інформаційної безпеки і зниження рівня цієї безпеки в противника. Поставлена мета може бути досягнута вирішенням ряду взаємопов'язаних завдань, найважливішими з яких будуть руйнування інформаційного поля супротивника і збереження свого інформаційного поля.

Перший досвід ведення інформаційного протиборства як однієї зі складових воєнного протиборства, був набутий у війні в зоні Перської затоки. Тоді багатонаціональні сили, використовуючи методи радіоелектронної протидії, здійснили блокування практично всієї інформаційної системи Іраку. Цей успіх не тільки окрилив США в розумінні ролі інформаційного протиборства, а й змусив замислитися над тим, як вийти з подібного становища, коли таке протиборство буде нав'язане їм самим. Були проведені аналітичні дослідження й експерименти під керівництвом агентства інформаційної безпеки Міністерства оборони США, які виявили, що ступінь уразливості комп'ютерних систем і баз даних військового відомства США є надзвичайно високим. Проникнути в мозковий центр Пентагона виявляється не складно, тому що він має множину виходів в інші інформаційні системи як усередині країни, так і за її межами.

На відміну від інших форм і способів протиборства інформаційне протиборство ведеться постійно в мирний час і справляє прямий і безпосередній вплив практично на всі сторони підготовки і ведення бойових дій у воєнний час. Виявляється, найбільш просто проникнути в інформаційні мережі країни можна, крім традиційних каналів радіо, телебачення, засобів масової інформації, через канали Інтернету. Через ці ж канали можна без усяких свідків здійснювати психологічний вплив на супротивника, а свою країну заздалегідь попереджати про загрозу її національним інтересам. Доступність глобальної комп'ютерної мережі дає змогу передавати необхідну інформацію в будь-який регіон світу, і можна виконувати багато завдань, пов'язаних з інформаційним протиборством.

У наш час інформаційне протиборство вже стало найважливішим змістом війни, але через застосовувані в ньому сили і засоби, а також специфічні цілі й завдання набуває як значної самостійності, так і є невід'ємним елементом усіх інших форм боротьби.

1.4. Інформація, інформаційна діяльність та її форми на сучасному етапі розбудови державності

1.4.1. Сутність понять «інформація» та «інформаційні ресурси»

Визначення поняття «інформація», попри його давнє походження, трансформувалося в міру розвитку людського суспільства. До початку 1940-х років під інформацією розуміли відомості, які передаються людьми усно, письмово або іншим способом. Вважається, що термін «інформація» походить від латинського *informatio* — роз'яснення, викладення. У сучасному його визначенні проглядається дихотомія: по-перше, це деякі відомості, сукупність якихось даних, знань і, по-друге, це одне з основних понять кібернетики.

Наукове визначення поняття інформації дало змогу підійти єдиного погляду на різні процеси, а саме: на передавання відомостей по технічних каналах зв'язку, функціонування нервової системи, роботи обчислювальних машин, різних процесах управління і т. ін. — всюди маємо справу з процесами передавання, збереження й перероблення інформації. Поняття інформації відіграло таку саму роль, як і поняття енергії в фізиці, воно надає можливість з загальної точки зору описати різні фізичні процеси⁴⁸.

Арістотель розрізняв внутрішню і зовнішню інформацію в системі. В поняття внутрішньої інформації (інформація як характеристика організованості системи) він вкладав сенс активного початку, який перетворює можливість на дійсність⁴⁹, яку сучасна наука визначає як міру організації системи і яка має назву «структурна інформація». Структурна інформація притаманна всім об'єктам живої і неживої природи, природного й неприродного походження і виникає як результат відбору, фіксації й закріплення в системі у формі визначених структурних змін її позитивного досвіду обміну із зовнішнім середовищем. Ця інформація має відносну об'єктну самостійність.

Математичне вираження «інформації» тотожне вираженню «ентропії», взятої з протилежним знаком⁵⁰. Тобто, якщо ентропія системи виражає ступінь її невпорядкованості, то інформація надає міру організації системи.

Зовнішня інформація — це інформація як засіб організації будь-якої системи, в сучасній науці має тлумачення «відносна інформація» (інколи тлумачиться як оперативна, робоча інформація). Ця відносна інформація завжди пов'язана з відношенням двох певних процесів.

Припустимо, що ми маємо два процеси А і В із множиною різних станів. Якщо кожному стану в А відповідає визначений стан в В й відношення між станами в В є ізоморфними відношенням між станами в А, то можна сказати, що процес В несе інформацію про процес А⁵¹.

Нагадаємо, що ізоморфізм (*грецьк.* — однаковий, рівний за формою) — це відношення між об'єктами, які мають однакову структуру. Дві структури (системи або множини) є ізоморфними одна до одної, якщо кожному елементові першої структури відповідає лише один елемент другої і кожній операції (зв'язку) однієї структури відповідає операція (зв'язок) в іншій та навпаки⁵².

Інформація є одним з основних понять у кібернетиці. Ця наука як відносно нова галузь знання народилася на основі теорії інформації, теорії алгоритмів, теорії ігор, теорії автоматів і дістала своє ім'я від давньогрецького слова «кібернетос», що в перекладі означає «керуючий», «кормач», тобто кібернетика — це наука про управління. «У загальному вигляді процес самоуправління в будь-якій самодіючій системі, — писав академік В. М. Глушков, — складається з трьох стадій: система вивчає обстановку, потім виробляє тактику дій (у механізмі вона міститься у вигляді програми) і тільки потім приймає рішення, як досягти мети. Їх виконання починається з передачі команди і супроводжується контролем за ходом виконання»⁵³.

У контексті теми нашої роботи і для розуміння ролі інформації в біосистемах важливо зазначити, що виділення інформації навколишнього середовища здійснюється біосистемами двома способами: перший — за допомогою енергоінформаційної взаємодії з навколишнім середовищем і другий — шляхом суто інформаційної взаємодії. У першому випадку енергія, яка поглинається біосистемою, є одночасно й носієм інформації, що спрацьовує як сигнал, котрий викликає реакцію біосистеми за рахунок її власних енергетичних ресурсів. У другому — це суто

інформаційна взаємодія, відокремлена від енергетичного обміну. Важливо відмітити, що за суто інформаційної взаємодії енергетичний ефект реакції біосистеми значно перевищує енергію самого інформаційного сигналу.

У біологічних і соціальних системах відрізняють три форми інформації, які відповідають трьом фізичним сутностям кібернетичних систем: біологічна (всередині живих організмів і між ними, у тому числі генетична, зоопсихологічна), машинна (всередині й між машинами), соціальна (в людських суспільствах).

Кібернетика має безпосереднє відношення до процесів управління й пізнання. Саме кібернетичні системи здатні до формування оптимальної поведінки в середовищі свого існування, де вона має постійно пристосовуватися до умов, які безперервно змінюються, досліджуючи, вивчаючи і впізнаючи це середовище шляхом збору і обробки як зовнішньої, так і внутрішньої інформації, в результаті чого формується динамічна інформаційна модель навколишнього середовища. Тому *необхідною умовою* будь-якого процесу управління та/або процесу пізнання, які відбуваються в живому організмі, в технічній системі або людському суспільстві, є процеси збору, накопичення, переробки й поширення інформації в процесах вироблення управляючих впливів для досягнення цілей керованої системи, і будь-яке втручання в ці процеси призводить до небажаних результатів у функціонуванні зазначених систем.

Є кілька визначень поняття «інформація». Зокрема, ЮНЕСКО надає таке визначення: *інформація — це «універсальна субстанція, яка проймає всі сфери людської діяльності, і слугує провідником знань та думок, інструментом спілкування, взаєморозуміння й співробітництва, утвердження стереотипів мислення й поведінки»***.

Під інформацією Закон України «Про інформацію» (ст.1) розуміє *«документовані або публічно оголошені відомості про події і явища, що відбуваються в суспільстві, в державі та навколишньому природному середовищі»*[^].

Довідник «Інформаційні ресурси Росії» надає таке тлумачення: «Інформація — це відомості про осіб, предмети, факти події, явища й процеси, незалежно від форми їх подання»⁵⁶.

Тобто *інформація — це відомості про факти, події, явища, процеси, які передаються в просторі й часі та використовую-*

ються з метою збереження або отримання знань, прийняття рішень, забезпечення функціонування суспільства.

У найзагальнішому вигляді інформація як така забезпечує задоволення інформаційних потреб суспільства і його суб'єктів у всіх сферах життєдіяльності, створення на цій основі сприятливих соціально-економічних і екологічних умов життя населення.

Науково-технічна інформація (НТІ), яка отримується в процесі наукової, науково-технічної, виробничої та громадської діяльності та містить відомості про досягнення науки, техніки, економіки та виробництва, Законом України «Про інформацію»⁵⁷ визначена як окрема галузь. Закон України «Про науково-технічну інформацію»⁵⁸ визначає: «*Науково-технічна інформація* — це документовані або публічно оголошені відомості про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержувані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності», «*Науково-технічна інформація охоплює в процесі науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності результати, зафіксовані у формі, яка забезпечує їх відтворення, використання і поширення. Науково-технічна інформація є суспільним надбанням, необхідною умовою продуктивної інтелектуальної діяльності, зокрема наукової і технічної творчості*».

За своєю роллю у правовій системі інформація поділяється на *нормативну правову інформацію* і *ненормативну правову інформацію*. Перша створюється у порядку правотворчої діяльності і міститься в нормативних правових актах; друга — як правило, — в порядку правозастосовної та правоохоронної діяльності, за її допомогою реалізуються положення правових норм. Ненормативна правова інформація створюється в об'єкті управління й рухається в контурі зворотного зв'язку системи правового регулювання.

У більшості розвинутих економік світу інформація вже стала центральним ресурсом як найбільш потужне джерело додатної вартості у виробництві та у сферах послуг, адміністративного управління та досліджень. Здатність до управління інформаційними ресурсами чим далі настійливіше визначатиме відмінність між успіхом та невдачею для організацій, окремих

соціальних та виробничих груп і навіть націй. Справедливим у такому контексті є також і те, що інформаційні технології мають справді базове значення і є важливим засобом, але капіталовкладення лише в інформаційну технологію або лише в інформаційні ресурси (а тим самим — і в інформаційну технологію як компоненту цих ресурсів) не є гарантією продуктивності та успіху. Ключовою проблемою стає стратегічне та економічне управління інформацією. Це в свою чергу потребує аналітичного підкріплення задля виявлення стратегічного застосування інформаційних ресурсів.

Враховуючи те, що національна безпека держави стає дедалі залежнішою від інформації, національні інформаційні ресурси держави можна умовно розподілити на кілька рівнів значущості, а саме:

Стратегічні інформаційні ресурси — життєво важливі інформаційні ресурси (з позиції національної безпеки), використання яких (без обмеження доступу, захисту, запобігання руйнуванню або знищенню) становить надзвичайну загрозу інтересам держави або навіть загрозу самому існуванню незалежної держави.

Критичні інформаційні ресурси — інформаційні ресурси, втрата яких завдає значних економічних, політичних або соціальних збитків державі (в разі їх розголошення, витоку або використання на шкоду суб'єктам правовідносин держави).

Цінні інформаційні ресурси — інформаційні ресурси, втрата або порушення цілісності яких пов'язана із значними втратами життєздатності систем управління економіки, науки, виробництва, господарської та комерційної діяльності підприємств та організацій усіх форм власності України.

Загальносуспільні інформаційні ресурси — інформаційні ресурси, які забезпечують загальні відносини в суспільстві, не мають ознак (у широкому розумінні) загроз державному суспільному ладу, державним інституціям, певним комерційним або господарюючим суб'єктам.

Інформатизація як технологічне використовує поняття «інформаційні системи», що являє собою сукупність технічних, програмних та інших засобів, поєднаних функціонально і структурно для забезпечення інформаційних процесів та надання інформаційних послуг⁵⁹.

Інформаційний масив являє собою впорядковану сукупність документованої інформації певної предметної сфери, зафіксованої на матеріальних носіях інформації з відповідним довідково-пошуковим апаратом та реквізитами, які дають змогу її ідентифікувати. Інформаційний пошук, надання змістовної інформації відбувається завдяки певним технологіям, виробничими засадами яких є *інформаційна техніка* — технічне обладнання та устаткування, що складає величезні системні комплекси, які оперують значними обсягами інформації та мають високий рівень інформаційної діяльності. Формування, зберігання, розвиток, поширення змістовних інформаційних ресурсів інформаційних масивів здійснюється в межах інформаційних інфраструктур, які об'єднують як неподільне системи, інформаційні технології та відповідні організаційні структури. Тобто в державі об'єктом управління може бути не інформаційний ресурс як такий, а організаційна побудова, інфраструктура, система «вкладених об'єктів»⁶⁰, у межах якої й здійснюється управління.

У результаті отримання, використання, поширення та захисту інформації виникають *інформаційні відносини* в політичній, економічній, культурній, соціальній, екологічній, науково-технічній, міжнародній та інших сферах життєдіяльності держави. Через інформаційні відносини, точніше, через їх упорядкування стосовно об'єкта зацікавленості виникає *інформаційна діяльність* — сукупність процесів збирання, аналізу, перетворення, зберігання, пошуку та поширення інформації, а також інших допоміжних процесів, що системно здійснюються будь-якою організацією (установою, підрозділом, групою осіб тощо). Оскільки в сукупності цих процесів інформація є основним об'єктом, їх називають інформаційними.

Інформаційна діяльність є складовою суспільного виробництва, пов'язаного з підготовкою інформаційних продуктів і послуг, спрямованих на задоволення суспільних потреб, вона передбачає виконання таких функцій, як: збір інформації, її опрацювання, формування інформаційних масивів, збереження і пошук, поширення інформаційних продуктів і послуг. В історії обміну інформацією людство переживає п'яту технологічну революцію, ті, що передували їй, пов'язані насамперед з винаходом у 1456 році Й. Гутенбергом друкарського верстата з рухливими металевими літерами, створенням О. Беллом у 1876 році

телефонного апарата, О. Поповим у 1895 році — радіо, Дж. Моклі і Д. Еккертом у 1945 році — першої ЕОМ і, кінець кінцем, технологій мобільних і глобальних комунікаційних мереж, які, синтезуючи знання в галузі зв'язку, об'єднують сьогодні величезний інформаційний масив, накопичений людством.

Інформаційна інфраструктура в процесі здійснення інформаційної діяльності, спрямованості на задоволення *інформаційних потреб* споживача, підпорядкована основному завданню — отриманню і доведенню до споживача *інформаційних продуктів та послуг* (ІПП) через визначений технологічний процес науково-інформаційної діяльності. Форма послуги може бути матеріальною або нематеріальною (підготовка і проведення конференцій, нарад, лекцій, консалтингу), та комбінованою (виставки нових надходжень, тематичної інформації, огляди та переклади за предметною галуззю знань).

Інформаційна діяльність — це діяльність суб'єктів. Термін «суб'єкти інформаційної діяльності» (інформаційні органи) є узагальнюючим і однаковою мірою може бути застосований до таких організаційних структур, як державні органи, підприємства, установи і організації, їх спеціалізовані інформаційні підрозділи і служби, установи і підрозділи НТІ, інформаційні центри тощо. Сукупності організаційних структур з відповідним правовим, методичним, інформаційним, лінгвістичним, технічним і кадровим забезпеченням постійно здійснюють інформаційну діяльність, забезпечуючи покладене на них завдання надійного функціонування інформаційних систем, застосування інформаційних технологій для обслуговування інформаційних потреб особи, держави і суспільства. Ми маємо їх розглядати як основу інформаційної інфраструктури держави.

Глобалізація економічних і політичних процесів і інформатизація суспільного життя зумовлюють акцентування на умовах інтернаціоналізації інформаційної діяльності при формуванні так званого інформаційного суспільства, в якому одним із основних предметів праці більшої частини людей є інформація і знання, а знаряддям — інформаційні технології.

Уперше визначення «інформаційне суспільство» було введено в науковий ужиток у Японії в 1966 році в доповіді групи з наукових, технічних і економічних досліджень. У ньому стверджувалося, що інформаційне суспільство передбачає достатній

обсяг високоякісної інформації та всі необхідні засоби для її поширення⁶¹. Сьогодні проблемам розвитку і становлення інформаційного суспільства присвячено багато наукових праць, зокрема українських фахівців і вчених⁶².

Можна стверджувати, що інформаційне суспільство має такі відмітні ознаки, як-то: інформація використовується як один із економічних ресурсів з метою підвищити ефективність виробництва, зміцнити конкурентоспроможність, стимулювати інновації; вона формує інформаційний сектор в економіці, який зростає швидше від інших, стає предметом масового споживання суспільства, формуючи ринок глобального інформаційного середовища, де відбуваються процеси обміну інформаційними продуктами і послугами.

Вочевидь, що й у новій інформаційній економіці незабаром буде впроваджений поділ на «сировинну» й «обробну» галузі. «Сировинний» сектор оброблятиме масиви неопрацьованої інформації, які зберігаються в архівах і бібліотеках або постачаються глобальними інформаційними мережами. «Обробний» сектор із спеціалізованими структурами перетворюватиме часто безсистемні дані на змістовну інформацію, яка зумовлює науково-технічний і загалом освітній і промисловий потенціал країн. Тому входження в глобальне інформаційне середовище не відміння наявності національних інтересів і необхідності забезпечувати їх безпеку.

1.4.2. Модель інформаційної сфери

З ускладненням організаційної структури суспільства управління в сучасному світі стає дедалі важчою справою. Це зумовлено насамперед характером відносин між різними елементами суб'єктів інформаційної діяльності й зовнішнім стосовно них середовищем. Тому для розгляду суспільних відносин, пов'язаних з інформацією та її обігом, сформуємо модель інформаційної сфери. За Р. Шенноном, «модель є відображенням об'єкта, системи або поняття (ідеї) в деякій формі, яка відрізняється від форми їхнього реального існування. ...Модель — це використовуваний для передбачення й порівняння інструмент, який дає змогу логічним шляхом спрогнозувати наслідки альтернативних дій та достатньо впевнено вказати, якому з них надати перевагу»⁶³. Людство протягом тисячоліть використовувало концепцію

моделі, намагаючись уявити й відобразити за їх допомогою абстрактні ідеї та реальні об'єкти.

Відомо, що будь-яка модель являє собою в загальному вигляді комбінацію таких складових, як компоненти, змінні, параметри, функціональні залежності, обмеження, цільові функції.

Інформаційна сфера може розглядатися як сфера діяльності, пов'язана зі створенням, поширенням, перетворенням і використанням інформації, а *інформаційні процеси* мають охоплювати процеси як виробництва, передавання, пошуку, одержання і поширення інформації, так і створення і застосування інформаційних систем, інформаційних технологій та засобів їх забезпечення. Саме при виконанні інформаційних процесів виникають суспільні відносини, що потребують правового врегулювання в інформаційній сфері, які називають *інформаційними відносинами*, а діяльність по здійсненню інформаційних процесів є *інформаційною діяльністю*.

Для дослідження інформаційних процесів суспільних відносин, що пов'язані з інформацією та її обігом, сформуємо модель інформаційної сфери (рис. 3).

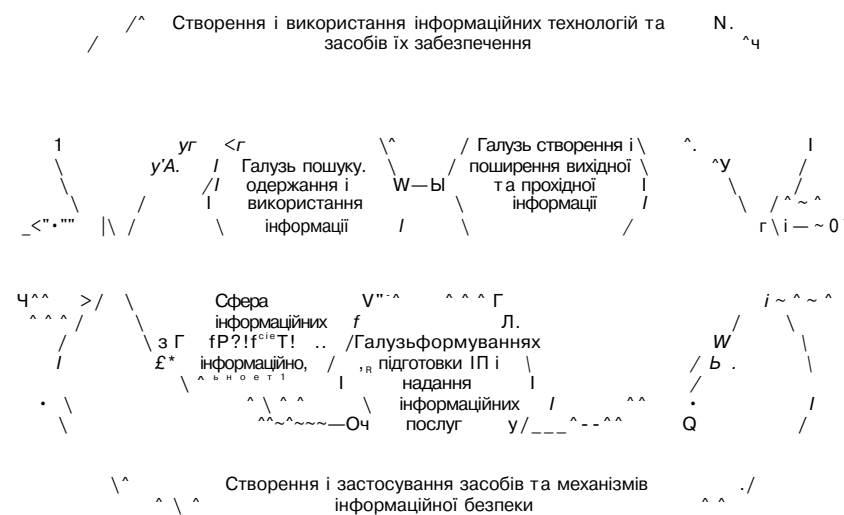


Рис. 3. Модель інформаційної сфери

Подана модель інформаційної сфери формувалася в міру розвитку обчислювальної техніки і технології оброблення інформації, розвитку мережевих технологій, удосконалення організаційних форм суб'єктів інформаційної діяльності протягом десятиліть. І якщо уважно придивитися до організаційної структури автоматизованої системи управління виробництвом великого машинобудівного підприємства 1980-х років (наприклад, київського державного авіаційного заводу «Авіант»), то побачимо в ній всі елементи зображеної моделі.

Інформаційну сферу умовно можна розподілити на основну частину, пов'язану безпосередньо з обігом інформації, — фігури I, II, III, які інтегровані фігурою А на рис. 3, і ту, що забезпечує цей обіг, — фігури В, С. У даній моделі немає зайвих або малозначущих елементів. Тому підкреслимо умовність поділу даної моделі на основну і забезпечуючу частини з погляду ефективності і надійності функціонування моделі в цілому — багаторічна практика свідчить, що нерозв'язаність проблем у забезпечуючій складовій інколи повністю блокує функціонування інформаційної системи в цілому.

Елемент II моделі реалізує функцію *створення і поширення вихідної і похідної інформації*, елемент III — *формування інформаційних ресурсів, підготовки інформаційних продуктів і надання інформаційних послуг*. Ці обидва елементи активно впливають на елемент III, функціональне призначення якого — *пошук, одержання і використання інформації*. Зазначені три елементи моделі інформаційної сфери утворюють сферу інформаційних процесів та інформаційної діяльності — фігура А.

Розвиток техніки зв'язку, обчислювальної техніки, мережевих технологій, поява нових носіїв інформації і способів її накопичення і обігу привів до появи елемента В моделі — *створення і використання інформаційних технологій і засобів їх забезпечення*, який забезпечує основні елементи можливостями програмно-апаратних засобів, засобів зв'язку та телекомунікацій. А поява таких нових для «старої» обчислювальної техніки явищ, як «віруси», несанкціонований, у тому числі дистанційний, доступ до накопиченої в «пам'яті» ЄОМ інформації, потребувала зосередження уваги на проблемах інформаційної безпеки, в результаті чого в інформаційній моделі набув розвитку елемент

С — *створення і застосування засобів і механізмів інформаційної безпеки*.

Усі елементи поданої моделі постійно розвиваються і впливають на розвиток і функціонування один одного. Вихідна інформація створюється під впливом навколишнього середовища, а також на базі використання інформаційних ресурсів, які в свою чергу формуються на основі вихідної і похідної інформації, насамперед як джерело ретроспективної інформації. У результаті опрацювання інформації створюється нова вихідна і похідна документована інформація, формуються і поповнюються інформаційні ресурси. Таким чином, і в найзагальніших рисах здійснюється обіг інформації в інформаційній сфері, схематично змодельованій нами.

1.4.3. Інформатизація науки і глобальний інформаційний простір

Наука, основним результатом діяльності якої є нові знання про оточуючу нас дійсність, має особливе значення для різних сфер загальнолюдської діяльності. Однак в українському суспільстві поки що не склалося розуміння того, що наука гарантує сам факт існування і стійкого розвитку держави, визначає її майбутнє.

Показовим у зв'язку з цим є розгляд співвідносин у тріаді «наука — техніка — виробництво». Досвід розвитку науково-технічного прогресу в розвинутих країнах світу (і вітчизняний також) дає змогу сформулювати такий принцип: для ефективного розвитку матеріального виробництва темпи розвитку науки і технологій мають перевершувати темпи зростання виробництва, а наука у своєму розвитку — випереджати темпи розвитку техніки та технологій.

Ще в 1939 році цей принцип був сформульований англійським наукознавцем Дж. Берналом у праці «Соціальна функція науки»: «Наука має розглядатися як друга похідна від загального продукту. Справжня продукція може слугувати точкою відліку в судженнях про фінансування науки. Розширення чи поліпшення виробництва звичайними технічними методами є першою похідною. Нею представлена швидкість виміру існуючих процесів виробництва. Друга похідна — швидкість зміни

першої — саме це і є те, що робить наука»⁶⁴. Іншими словами, розширення чи поліпшення виробництва звичайними технічними методами є першою похідною — як відомо, першою похідною від пройденого шляху є швидкість, а другою — прискорення («швидкість зміни першої»). Тобто саме наука забезпечує прискорення в економіці. Доки на вищих рівнях прийняття політичних рішень це положення не буде усвідомлене, будемо мати те, що маємо, а далі — гірше.

Тому особливість підтримки науки державою полягає насамперед у спрямуванні наукових досліджень, удосконаленні їх організації, а також питаннях фінансування розвитку науки, техніки й технологій.

На підтвердження думки про випереджальну роль розвитку науки в суспільстві наведемо слова видатного фізика, лауреата Нобелівської премії академіка М.М. Семенова: «...Головною особливістю науки ХХ століття є та обставина, що вона перестала бути тільки служницею виробництва, а перетворилася на матір виробництва... Наука, що розкриває таємниці природи (будемо називати її фундаментальною), породжує лише основи техніки, подальший розвиток якої забезпечується відповідною прикладною наукою і технікою. Це вони, в остаточному підсумку, перетворюють відкриття науки на могутні сили виробництва»⁶⁵.

Людство перебуває на порозі інформаційного суспільства, в якому провідну роль починає відігравати нова сфера — інформаційна галузь, одним із основних факторів якої є наука. У зв'язку з цим доцільно нагадати, що стосовно інформаційного суспільства іноді використовують термін «суспільство, засноване на знаннях». І коли академік М.М. Моїсєєв, міркуючи про майбутнє Росії, стверджує, що могутність держави на цьому етапі визначатимуть не снікери і памперси і навіть не виробництво електроніки, а «виробництво ідей», тобто наука, то автор поділяє саме такий підхід до проблеми.

На жаль, нашим науковцям доводиться постійно нагадувати уряду про важливість для держави своєї роботи і переконувати його в необхідності збільшення фінансування науки замість нинішніх 0,3% ВВП до 1,7% з наступного року, а в подальшому — 2,4% , як це передбачено законодавством України⁶⁶.

Парадокси в різних сферах життєдіяльності нашого суспільства свідчать не про окремі помилки, а про системну кризу, корені якої — у нашому світорозумінні, що виявилось неадекватним об'єктивним реаліям.

Тим часом будь-яке управлінське рішення на будь-якому шаблі має об'єктивно укладатися в русло тієї чи іншої концепції, поза залежністю від того, усвідомлюється воно чи ні як особами, котрі приймають рішення, так і тими, чий інтереси воно зачіпає. Але ж в основі формування цілей розвитку, концепцій управління лежить світогляд як їх система координат і точка відліку. Саме моральністю і світоглядом значною мірою визначаються суспільний добробут, рух до достатку, довготермінові перспективи будь-якої з країн і навіть цивілізацій. «Світогляд визначає не тільки внутрішні взаємовідносини в суспільстві, а й ставлення до навколишнього світу, і характер його впливу на таке суспільство у відповідь. ...Можна мати психологію маленьких людей ... і вважати нормою їх підпорядкування оточуючим... Злиденне існування володарів таких світоглядних систем гарантоване їм на століття»⁶⁷.

Найважливішою якістю, яку треба мати вектору цілей державного управління, всім без винятку стратегічним цілям, є чітка концептуальна визначеність. Якщо суспільство демократичним шляхом сформувало вектор цілей управління, то з цього моменту визначаються ясні функції тих, хто стоїть біля керма управління державою.

Проблема саме в тому, що весь інтелектуальний ресурс країни, за відсутності єдиної для всіх довготермінової загальнодержавної стратегії розвитку і відповідної концепції управління, зосереджений на оптимізації окремих суперечливих рішень. При цьому ми навіть не усвідомлюємо наявності визначеної методології глобального, наддержавного управління, яке реалізується щодо кожного окремого суб'єкта управління і державності в цілому.

Так, за відсутності такої концептуальної визначеності в систематизації законодавства в Україні як важливому чиннику розвитку правової системи будь-якої держави за 12 років її незалежного розвитку не спостерігається особливого (окрім прогресу, певно, факту прийняття нової Конституції України). Як зазначають автори монографії «Систематизація законодавства Украї-

ни: проблеми та перспективи вдосконалення», «навпаки, законодавчий масив безсистемно розширюється, розгалужується, стає більш заплутаним та невпорядкованим»⁶⁸.

Отже, інтенсифікація науки і підвищення її ефективності є надзвичайно актуальною проблемою суспільного розвитку, розв'язання якої неможливе без інформатизації науки як основи підвищення ефективності наукових досліджень, прискорення процесу одержання і поглиблення наукових знань про явища і закономірності в природі, техніку і суспільство шляхом активного використання нових інформаційних засобів і технологій на всіх етапах наукової праці. Інформатизація науки за своєю суттю спрямована на максимальну автоматизацію цих інформаційних процесів, що досягається створенням комп'ютерних автоматизованих систем наукових досліджень, якщо їх розглядати, зокрема, у вигляді комплексів автоматизованих робочих місць, які забезпечують пошук і аналіз первинної інформації (першоджерел), автоматизацію теоретичних і експериментальних робіт, документування, прискорення підготовки звітів і наукових праць і та ін. Пріоритетним напрямом інформатизації науки є створення локальних інформаційних мереж з розподіленими базами і банками даних, знань, документальною і фактографічною інформацією, інтелектуальними інформаційно-пошуковими системами із забезпеченням виходу цих мереж у регіональні, державні і міжнародні комп'ютерні мережі. Це дає змогу:

- радикально змінити стиль і рівень наукової праці, прискорити одержання нових знань, підвищити їхню вірогідність і якість;
- одержати оперативний доступ до наукових інформаційних фондів регіону, країни, світу;
- ліквідувати інформаційну ущербність «периферійних» країн і регіонів, різко активізувати їхню наукову діяльність;
- близити в часі й у просторі учених різних країн і регіонів, прискорити обмін науковими знаннями між ними і та ін.⁶⁹

Комп'ютерні мережі породили не тільки нові форми наукової комунікації (електронна пошта, телеконференції, електронні журнали, інтерактивний доступ до віддалених інформаційних і обчислювальних ресурсів, дистанційна участь в унікальних експериментах, телеробота по розподіленому виконанню спільних наукових досліджень і т.д.) і привели до інтенсифікації наукової

діяльності, а й відіграли, можна сказати, революційну роль у формуванні нових механізмів функціонування науки в цілому, створили нове інформаційне середовище, що зумовлює кардинальні зміни соціально-пізнавальних і комунікаційних основ науки.

Однією з перших глобальних інформаційно-обчислювальних мереж у СРСР була Академмережа, яка створювалася в 1980-х роках як комп'ютерна мережа з комутацією пакетів, орієнтована на використання міжнародних протоколів обміну даними. Розпад СРСР і наступна економічна криза призвели до того, що розвиток Академмережі до кінця 80-х років зупинився, а в 1991 році мережа фактично припинила своє існування. Проте Академмережа відіграла дуже важливу роль у становленні комп'ютерної мережної технології, вона стала полігоном по відпрацюванню базової мережі передачі даних, у процесі її створення були освоєні міжнародні протоколи обміну даними, і, що важливо, підготовлені фахівці з комп'ютерних мереж, досягнуто взаєморозуміння між фахівцями з мереж зв'язку і фахівцями з обчислювальної техніки, а користувачі одержали практичний досвід роботи в комп'ютерних мережах.

Академмережа значною мірою була провісницею епохи Інтернету, початок якої можна віднести до другої половини 80-х років. Слід зазначити, що академічне співтовариство відіграє важливу роль у розвитку Інтернету практично в усіх країнах світу. Саме завдяки цьому нині ця глобальна мережа стала фактично міжнародною мережею, що забезпечує можливості обміну інформацією в планетарному масштабі й утворює програмно-апаратну основу глобального інформаційного простору, а зміна ролі інформації в житті людства поряд з появою новітніх технологій її обробки, передачі, збереження й представлення зумовлює характерні риси сучасної цивілізації й появу нового середовища її функціонування — глобального інформаційного простору.

У його умовах кожна держава не може нехтувати необхідністю адаптації до цього віртуального середовища, оскільки від того, як така адаптація відбуватиметься, залежатимуть фактично всі параметри «державного здоров'я».

У вітчизняній і зарубіжній дослідницькій літературі вже зверталася увага на зв'язок інформації і розвитку інформаційних технологій з економічним розвитком суспільств і держав, з мож-

ливостями маніпулювання суспільною свідомістю, із бурхливим розвитком так званої масової культури, що дедалі інтенсивніше витісняє національну самобутність народів⁷⁰.

Стратегічну орієнтованість діяльності держави на нове середовище зумовлюють, на нашу думку, такі обставини.

Це, по-перше, зміна уявлень про співвідношення факторів могутності держав. Тривалий час вважали, що саме військова сила визначає рівень могутності держави. А в XX столітті ми вже спостерігали висування на перший план економічної сили як головного фактору могутності держави (наприклад, Японія і так звані нові індустріальні країни). Нині складається нове уявлення про головний чинник могутності держави. Згідно з таким уявленням головним фактором могутності держави в XXI столітті є інформація, здатність держави мати у своєму розпорядженні найсучасніші інформаційні технології і засоби, що дають змогу ефективно обробляти, зберігати, передавати й представляти необхідну інформацію. Володіння державою такою здатністю — шлях до подальшого нарощування на нових засадах своєї економічної й військової міцності.

По-друге, це формування третьої основи єдності людства — інформаційної єдності (поряд з економічною й екологічною). Сучасні технології обробки, систематизації, збереження й передачі інформації настільки швидкоплинні, що обсяги інформації, якими може оперувати сучасна людина, стали практично безмежними. Крім того, сучасні інформаційні технології стають дедалі доступнішими для кожної окремої людини. За прогностичними оцінками дослідників, до середини наступного століття в інформаційному плані для людини стануть доступними практично всі куточки світу. Можна буде за лічені хвилини передати й одержати необхідну інформацію в будь-якому можливому форматі її організації (текстовому, графічному, звуковому та ін.). Багато фахівців з вивчення проблем інформатизації суспільства цілком обґрунтовано стверджують, що ми є учасниками й свідками формування нової сфери єдності людства — інформаційної.

Економічна, екологічна й інформаційна єдність людської цивілізації альтернативні за своїми наслідками й за своєю природою. Глобальна інформатизація об'єктивно нестиме в собі добро і зло водночас. Оскільки окрема особа — індивід дедалі почу-

вається недієздатною, щоб повноцінно співвідноситися з навколишнім інформаційним середовищем, зір і слух зазнають страшенного навантаження, якого не витримують мозок і серце.

Це явище слід вважати «постмодерною травмою», що викликана диспропорцією між людиною, чиї можливості біологічно обмежені, і людством, яке необмежене у своїй техно-інформаційній експансії, причому воно має тенденцію до зростання. Тому, безперечно, для мінімізації їх негативних і посилення позитивних наслідків необхідно всебічно, комплексно і науково досліджувати в суспільстві гуманітарні, медико-біологічні, соціальні й інженерно-технологічні проблеми, розвивати природознавчі науки. Вочевидь, що міжнародному співтовариству реально необхідно досягти чіткого розуміння проблеми глобальної взаємозалежності національних інформаційних ресурсів у всій її повноті і комплексності, визнати, що успіх національних зусиль по охороні свого інформаційного ресурсу залежить від рівня захищеності і «неагресивності» інформаційних просторів інших, у тому числі несусідніх, держав, із якими їхні інформаційні ресурси об'єктивно пов'язані.

По-третє, Україні необхідно коректно освоювати глобальний інформаційний простір. Цей простір, як і будь-яке нове невідоме середовище, таїть у собі багато небезпек, про багато з яких ми можемо й не знати сьогодні. Глобальний інформаційний простір як середовище існування і функціонування народів і держав здатний як забезпечити й збагатити Україну великими ресурсами, так і призвести до зникнення національної культури, втрати народами України своєї національної самоідентифікації⁷¹.

В умовах глобалізації інформаційного суспільства, коли суб'єкти, інформаційні ресурси, канали зв'язку, системи, що рознесені в просторі і знаходяться на території різних держав або адміністративних утворень, виникає проблема, яке законодавство варто застосовувати при їхньому регулюванні.

У даний час кілька десятків країн світу мають досить розвинуте інформаційне законодавство, в тому числі таке, що має предметом свого регулювання глобальний інформаційний простір, прийняті (поки що дуже нечисленні) міжнародні угоди, проте дотепер немає єдиних підходів і рішень.

З огляду на викладене найпринциповішими проблемами регулювання в Україні правовідносин в інформаційній сфері є невизначеність або велика розбіжність у розумінні та практичному застосуванні таких системоутворюючих понять для системи інформаційного права, як «інформаційний суверенітет України», «інформаційний простір України», «інформаційна безпека України», «правовий режим інформації», «принципи міжнародного інформаційного співробітництва» тощо. Без визначення на рівні актів законодавства цих важливих політико-правових понять та правових норм щодо їхнього забезпечення неможливе встановлення цивілізованих міжнародних інформаційних відносин і подальше системне вдосконалення інформаційного законодавства України.

1.4.4. Національний інформаційний простір

Головним об'єктом, на який має бути спрямована дія Концепції національної інформаційної політики, є національний інформаційний простір (НІП) України. Вельми важливим є визначення місця і ролі інформаційного простору у системі суспільних відносин, оскільки він є необхідною умовою існування суспільства, субстанцією, де накопичуються суспільні знання, унормовуються суспільні відносини окремої людини з іншими людьми, спільнотами та державою.

НІП є складним багаторівневим і різнобарвним матеріальним утворенням, на тлі якого виникають, розвиваються і зникають цивілізації. Його складовими є історичне територіально розподілене нашарування інформаційних ресурсів та інформаційних технологій, що обслуговують процеси створення, зберігання та споживання інформації. Тобто глобальний інформаційний простір (ІП) є композицією інформаційних ресурсів, які утворені регіональними спільнотами, окремими країнами, міжнародними організаціями, релігійними течіями тощо.

Фундаментальною властивістю ІП є його недосконалість, тобто невідповідність реальних подій і явищ записам про них, з погляду повноти, адекватності та оперативності, перманентне відставання інформаційної пропозиції від нагальної суспільної потреби. Ступінь цієї невідповідності є характеристикою інформаційної безпеки суспільства, країни, окремої людини. Тому

досягнення абсолютної інформаційної безпеки доцільно розглядати як стан ідеального суспільства, як прагнення, що базується на відповідних концептуальних засадах.

Водночас збільшення кількості населення, розподіл і спеціалізація виробничих відносин, урізноманітнення номенклатури товарів і послуг вичерпують поточні можливості ІП обслуговувати сталий розвиток суспільства, консервують стан суспільних відносин. Країни, неспроможні утримувати стан інформаційної безпеки власного ІП на рівні розвинутих країн, опиняються у несприятливих умовах, насамперед у конкурентних змаганнях за розподіл ринків, ресурси, добробуту власного населення тощо. Як свідчить історія, навіть потужні в минулому імперії, зникли з сучасної мапи саме через неспроможність ефективного управління на власній території, невідповідність власного ІП новим потребам. І навпаки, широке запровадження новітніх інформаційних технологій є необхідною умовою економічного зростання окремих країн і навіть континентів. Наприклад, середньовічному ренесансу Європи сприяли передусім винахід і поширення книгодрукування як потужної інформаційної технології поширення знань та унормування суспільних відносин.

З іншого боку, ІП є потужним інструментом впливу на формування світогляду, моральних норм і цінностей окремих особистостей, відносин у виробничій сфері, побуту, правил суспільної поведінки тощо.

Але головною функцією ІП є обслуговування сучасних та розвиток майбутніх суспільних відносин, від яких залежить подальший розвиток або стагнація як окремих країн, так і цивілізації в цілому. Тому кожна країна змушена самостійно та у співпраці з іншими розвивати національний інформаційний простір (НІП), намагаючись зайняти гідне місце у світовому поділі праці та ресурсів, у конкурентній боротьбі за ринки збуту товарів та послуг, захищаючи власні національні інтереси.

Іншою фундаментальною властивістю інформаційного простору є обмеженість його розвитку екстенсивним шляхом, тобто простим нарощуванням та інтенсифікацією існуючих інформаційних технологій. Перехід суспільних відносин на новий щабель суспільного розвитку відбувається після радикальної надбудови усталених технологій створення, зберігання і споживан-

ня інформації новітніми, що спираються на відкриття і застосування нових фізичних принципів реєстрації інформації, досягнення точних наук.

Зокрема, передача інформації за допомогою штучного електромагнітного випромінювання стала надбанням інформаційних технологій початку минулого століття, а створення, зберігання і споживання інформації за допомогою комп'ютеризованих систем та утворення глобальної мережі інформаційних ресурсів — головна інформаційно-технологічна спадщина нового тисячоліття.

Наступні кроки розвитку глобального інформаційного простору остаточно ще не визначені. Потенційна ємність новітнього інформаційного простору поки що суттєво перевищує виробничі можливості щодо його змістовного наповнення, контекстної структуризації. Натомість процедури пошуку необхідної інформації, її аналітичної обробки потребують дедалі більше часу і зусиль, що часто зводять нанівець потенційні можливості новітніх інформаційних технологій.

Тобто виникає комплексна проблема розробки нових принципів актуалізації національного Ш, зокрема фактографічного гатунку, з унормованим сенсом, достовірністю, періодичністю і щільністю для розв'язання завдань обліку, прогнозування, оптимального планування тощо. Для цього потрібні концептуальні цілеспрямовані зусилля держав щодо переведення сучасного інформаційного простору з засад мас-медійного зв'язу, розваг і проникнення реклами в суспільну свідомість на засади точного механізму управління, автоматизованого посередника кожного з кожним.

Завдання України на тлі інформаційної глобалізації ще складніші, оскільки, окрім участі в розробці нових принципів актуалізації новітнього національного ІП, вона має суттєво зменшити наявне відставання від розвинутих країн у сфері інформаційних технологій, опанувати і локалізувати існуючі технології, збільшити питому вагу і цінність національної складової глобального інформаційного простору.

У контексті зазначеного потребує негайного вирішення, поперше, визначення змісту поняття інформаційного суверенітету України і його правового режиму, оскільки в чинному законодавстві та законопроектах, що знаходяться на розгляді у

Верховній Раді України, містяться правові норми, які різняться як за змістом, так і за напрямками діяльності.

Так, у ст.1 Закону України «Про національну програму інформатизації»⁷² говориться, що інформаційний суверенітет держави — це «здатність держави контролювати й регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки». Таке визначення поняття інформаційного суверенітету суперечить нормам ст. 53 Закону України «Про інформацію»⁷³ та ст.23 Закону України «Про науково-технічну інформацію»⁷⁴, якими встановлено, що основою інформаційного суверенітету є національні інформаційні ресурси.

У ст. 2 проекту Закону України «Про інформаційний суверенітет та інформаційну безпеку України»⁷⁵ інформаційний суверенітет визначено як «право держави на формування і здійснення національної інформаційної політики відповідно до Конституції й законодавства України, міжнародного права в національному інформаційному просторі України». За своїм змістом це поняття не є вичерпним, бо не враховує глобалізаційних процесів в інформаційній сфері та розвитку міжнародного інформаційного співробітництва суб'єктів України (фізичних і юридичних осіб, держави).

Окрім того, аналіз публікацій у пресі та деяких періодичних видань свідчить про те, що в Україні є як прибічники, так і супротивники визначення у правовому плані поняття «інформаційний суверенітет» та правових норм його забезпечення.

На нашу думку, інформаційний суверенітет є похідним від державного суверенітету, але не є рівнозначним йому. До формування поняття «інформаційний суверенітет» доцільно підходити, виходячи з того, що суверенітет — це верховна влада у внутрішніх справах і незалежність у зовнішніх відносинах. При цьому необхідно враховувати, що інформаційний суверенітет з пргляду політико-правового навантаження має подвійний характер: з одного боку, це виключне право держави та її можливості, з іншого — це основні функціональні напрями (завдання) державної діяльності.

На нашу думку, інформаційний суверенітет України — це виключне право України відповідно до Конституції і законодавства України та норм міжнародного права самостійно і не-

залежно, з додержанням балансу інтересів особи, суспільства і держави визначати і здійснювати внутрішні й геополітичні національні інтереси в інформаційній сфері, державну внутрішню й зовнішню інформаційну політику, розпоряджатися власними інформаційними ресурсами, формувати інфраструктуру національного інформаційного простору, створювати умови для його інтегрування у світовий інформаційний простір та гарантувати інформаційну безпеку держави.

Вочевидь, що досі чинне законодавство не визначило правовий статус інформаційного простору України — важливу ознаку й передумову формування інформаційного суспільства, входження України у світове інформаційне співтовариство, один із головних чинників збереження інформаційного суверенітету, зміцнення державності та забезпечення національної безпеки України

У ст.4 проекту Закону України «Про інформаційний суверенітет та інформаційну безпеку України» запропоновано таку редакцію цього поняття: «Національний інформаційний простір України — сфера (об'ємний простір), у якій здійснюються інформаційні процеси і на яку поширюється юрисдикція України».

У проекті Концепції (Основах державної політики) інформаційної безпеки України, розробленій УЦЕПД ім. О. Разумкова, надано таке визначення: «Інформаційний простір України — середовище, в якому здійснюється продукування, зберігання та поширення інформації і на яку поширюється юрисдикція України»⁷⁶.

Обидві редакції поняття «інформаційний простір України», на нашу думку, не враховують основних елементів національного інформаційного простору та його функцій. А віднесення до національного інформаційного простору лише середовища, на яке поширюється юрисдикція України, є своєрідною перепорою для інтегрування у світовий інформаційний простір, де діють норми міжнародного права, відповідно до яких мають захищатися національні інтереси України.

Світовий досвід і сучасні вітчизняні наукові дослідження⁷⁷ свідчать про те, що сформулювати юридично обґрунтоване поняття «інформаційний простір України» можна, лише враховуючи сукупність елементів інформаційного простору держави та функціональні напрями державної діяльності, що охоплює

собою поняття «національний інформаційний простір» і виходячи виключно із суверенного права України на самостійне і незалежне вирішення цього питання.

На нашу думку, до основних ознак інформаційного простору України можна віднести:

- єдині принципи і загальні правила взаємодії всіх суб'єктів інформаційної діяльності при оптимальному співвідношенні державного регулювання і саморегулюючих засад у формуванні й розвитку інформаційного простору України;

- наявність умов для безпечної інформаційної взаємодії держави, організацій і громадян;

- максимально повне задоволення інформаційних потреб держави, організацій і громадян на всій території держави;

- рівний доступ суб'єктів інформаційної діяльності до відкритих інформаційних ресурсів та їхня правова рівність;

- збереження балансу інтересів держави і світового співтовариства при входженні України в глобальний інформаційний простір та забезпечення її національного інформаційного суверенітету.

Аналіз свідчить, що в процесі формування і розвитку інформаційного простору України мають бути досягнуті такі цілі, як:

- забезпечення конституційних прав громадян на інформацію;

- створення й підтримка інформаційного потенціалу, достатнього для стійкого й безпечного розвитку українського суспільства;

- забезпечення оперативного доступу до наявних інформаційних ресурсів та їхнє включення в інформаційний простір України за умов доступності до них на законній підставі органів державної влади, господарюючих суб'єктів і громадян;

- подолання інформаційного монополізму управлінських і комерційних структур на відкриті інформаційні ресурси — перехід від закритості інформації до її відкритості;

- підвищення рівня узгодженості рішень, що приймаються органами державної влади, регіональними (обласними) органами влади та місцевого самоврядування;

- надання можливості громадянам і громадським організаціям на законних підставах здійснювати контроль за діяльністю органів державної влади і місцевого самоврядування;

— підвищення рівня правосвідомості, ділової й громадськості активності громадян шляхом надання їм вільного доступу до правових і нормативних документів, які визначають їхні права і обов'язки, а також рівної можливості користуватися відкритою науково-технічною, соціально-економічною, суспільно-політичною інформацією, інформаційними фондами сфер освіти, культури та ін.;

— побудова інформаційного суспільства в Україні та її входження у світове інформаційне співтовариство за умов забезпечення захисту всіх елементів національного інформаційного простору, прав і свобод суб'єктів України, що діють у ньому, як важливого чинникові збереження інформаційного суверенітету України.

Оскільки національний інформаційний простір — важлива ознака суверенної й незалежної держави, яка дбає про формування й розвиток його на всій території України на основі єдиних принципів і за загальними правилами з додержанням балансу інтересів особи, суспільства, держави, на рівні законодавчого акта його слід визначити як сукупність національних інформаційних ресурсів та інформаційної інфраструктури, що дають змогу на основі єдиних принципів і загальних правил забезпечувати інформаційну взаємодію громадян, суспільства, держави з їх рівним правом доступу до відкритих інформаційних ресурсів та максимально повним задоволенням інформаційних потреб суб'єктів держави на всій її території з додержанням балансу інтересів на входження у світовий інформаційний простір та забезпечення інформаційної безпеки відповідно до Конституції України та міжнародних правових норм.

Є всі підстави вважати, що подальше зволікання з визначенням інформаційного простору держави не сприяє подоланню розбіжностей у розумінні різними політичними силами напрямів державної діяльності щодо його забезпечення та наближає Україну до критичної межі, за якою — втрата інформаційного суверенітету, неможливість захистити національні інформаційні ресурси, власну інформаційну інфраструктуру, свідомість суспільства від негативних інформаційних впливів як важливих складових національної безпеки держави.

Сукупність складних процесів і реакцій пристосування людини до комп'ютерного середовища, формування чіткого уяв-

лення про об'єкт інформатизації, алгоритмів її опрацювання машиною для потреб різноманітних соціально-економічних угруповань, гуманітарних, виробничих, наукових, комерційних завжди виявляє конкретну мету діяльності людини на кожному етапі роботи з інформацією: по-перше, збір і отримання інформації щодо окремого сегменту знань; по-друге, створення віртуального образу і кордонів маніпуляції з інформаційним ресурсом, перекладання на програму обраного алгоритму відображення реальності машиною відповідно до її можливостей опрацювати інформацію за заданим алгоритмом. На третьому етапі роботи людина має оцінити суб'єктивно отриманий через віртуальну систему інформаційний продукт, надавши йому достовірності, цінності, зокрема в грошовому еквіваленті, і включити його в обіг соціально-економічного середовища. Все це вимагає від людини високої кваліфікації, тому що на цьому етапі всі питання набувають яскравого суб'єктивного забарвлення: вибір засобів застосування інформаційного продукту, введення в обіг шляхом ринкового, службового, особистого застосування або подальшого опрацювання.

Сенс такої градації бачиться в тому, що, коли збір інформації користувачем є найбільш простим завданням, вирішується як за допомогою програмних і технічних засобів, то другий етап — застосування інформаційної технології значною мірою визначається цілями, сформованими на першому рівні.

Сьогодні не викликає сумнівів необхідність підвищення ролі науки, розвитку й ефективного використання інтелектуального та науково-технічного потенціалу для економічного і соціального розвитку держави. Проте ситуація у сфері науки не задовольняє суспільство, зокрема, набутий в Україні науково-технологічний потенціал поки що не вбудовується в запропоновані для його реформування бізнес-схеми і моделі, тенденцією стало порушення встановлених нормативів фінансування науки.

Розглядаючи тріаду «наука (фундаментальна) — наукова технологія — виробництво», побіжно підкреслимо, що перше з понять означає вид людської діяльності, призначений для виявлення невідомих законів природи і суспільства. Призначення технологій полягає у використанні вже відомих знань. А виробництво — то вже, власне, засіб тиражування досягнень технології.

Вочевидь, що межі всередині цієї тріади досить примарні. Проте функціональне призначення кожної з її складових цілком зрозуміле. Метод аналогій може прояснити цю суху матерію. Відмінність між наукою і технологією є приблизно L сі K сі, ЯК відмінність між розвідкою й головними військовими силами. Історія знає багато прикладів, коли відсутність розвідки або її погана організація шкодили армії навіть більше, ніж супротивник. Саме тому статuti всіх армій вказують на необхідність постійного ведення розвідки.

Представлена у вигляді інформаційних продуктів і послуг, призначених для здійснення процесів обміну на інформаційному ринку, наука є інтернаціональною за своєю природою, має соціально вагомий характер, не витрачається при споживанні, може породжувати якісно нову інформацію і використана необмежену кількість разів. Обмеженням на корисне використання інформації може бути тільки термін її старіння.

Інформаційні процеси перетворилися на предмет спеціального наукового осмислення в рамках математичної теорії інформації починаючи з 20-х років минулого століття, коли теоретики усвідомили існування складних систем, де зміна одного фактору стає причиною зміни інших, іноді дуже багатьох. Уже перші дослідження виявили невизначені закономірності, дефіцит наукових знань про природу і механізми виникнення, рух і споживання інформації.

Ускладнення загальної проблеми спричинило лавиноподібне наростання кількості науково-технічної інформації. Незважаючи на зростання попиту й удосконалення засобів його задоволення, очевидною стала неможливість практичного засвоєння людьми всього того, що виробляється і пропонується у вигляді інформації.

Теорія інформації, створена П.Флоренським, К.Богдановим, Н.Вінером, У.Ешбі, К.Шеноном, дала змогу виявити найзагальніші зв'язки, що проявляються в ході створення, передавання, прийому і споживання інформації в природі і суспільстві, вона надала дослідникам можливість за допомогою свого категорійного апарату максимально зосередитися на відносинах, що утворюють складні динамічні системи, які функціонують у постійно мінливому соціальному середовищі.

З огляду складність проблеми створення цілісної й дієвої системи управління національними інформаційними ресурсами, її комплексної реалізації вимагає з боку держави здійснення ряду заходів та прийняття нормативно-правових актів стосовно:

— порядку і правил формування, використання та захисту інформаційних ресурсів, що не містять інформації з обмеженим доступом;

— порядку й правил формування, поширення і захисту інформаційних ресурсів, що містять інформацію з обмеженим доступом;

— затвердження переліку документованої інформації, що в обов'язковому порядку надається для державної реєстрації (окремо — відкритої інформації і окремо — для інформації з обмеженим доступом);

— порядку і правил державного обліку та реєстрації баз і банків даних з урахуванням попередніх положень;

— встановлення відповідальності органів державної влади усіх рівнів щодо створення реальних можливостей для вільного і захищеного доступу до них.

Термінового вирішення потребує визначення критеріїв віднесення інформаційних ресурсів до категорії державних і створення правових механізмів регламентації порядку і правил роздержавлення інформаційних ресурсів, визначення механізмів забезпечення права на інформацію та свободи інформаційної діяльності.

Проголошене у статтях 9 і 10 Закону України «Про інформацію» право на інформацію та гарантії такого права не корелюються з обов'язками державних органів і юридичних осіб формувати інформаційні ресурси для відкритого доступу та з іншими їх повноваженнями й функціями. Чинне законодавство не містить норм впровадження правових та економічних механізмів міждержавного інформаційного обміну, зокрема щодо взаємодії інформаційно-телекомунікаційних систем України з глобальними інформаційними системами. Водночас і європейські норми вимагають сформувати в Україні систему відкритих державних інформаційних ресурсів, яка має містити в собі такі підсистеми: керуючу, нормативно-законодавчу, організаційно-методичну і виконавчу (центри, що засвідчують, зокрема, електронний нотаріат, якість, арбітраж).



В інтересах забезпечення інформаційної безпеки відкритих державних інформаційних ресурсів у складі комплексу робіт із створення основ їх формування й управління мають бути передбачені вибір стандартів обміну інформацією і розробка принципів забезпечення інформаційної безпеки процесів формування ВДІР і стратегії розвитку інфраструктури електронного документообігу загального призначення на загальнодержавному регіональному і муніципальному рівнях, а також управління ризиками (аудит, моніторинг, атестація, ліцензування, нагляд страхування).

Важливість використання при формуванні ВДІР уніфікованих захищених інформаційних технологій і важливості самої проблеми формування ВДІР у цілому зумовлює необхідність розробки Концепції формування і забезпечення доступу до державних інформаційних ресурсів, де комплексно мають бути розглянуті питання побудови і розвитку такої системи, визначені вимоги, яким мають відповідати інформаційні системи.

Уявити реальний обсяг роботи, яку потрібно виконати, можна на прикладі схеми формування інформаційних ресурсів для органів регіонального і муніципального управління Російської Федерації (рис. 4). Вочевидь, що існування такої складної системи взаємовідносин і підпорядкованості щодо використання національних інформаційних ресурсів матиме сенс тільки на підставі узгоджених засобів технічного забезпечення, нормативно-правових і організаційно-методичних засад. Тобто інфраструктура формування ВДІР має стати системою взаємопогодженої сукупності нормативних, законодавчих, методичних матеріалів, організаційних рішень і механізмів, технічних, програмних і технологічних об'єктів, які гарантуватимуть достатність використаної технології електронної взаємодії для визнання електронного документа юридичним фактом та забезпечуватимуть повноту, автентичність, доступність і актуальність інформації, а також її безпеку і вирішеність узгодження можливих конфліктів між учасниками електронної взаємодії.

1.4.5. Про правовий режим науково-технічної інформації

Правовий режим інформації та межі його дії є визначальною основою для встановлення інформаційної взаємодії між державною владою, особою і суспільством, важливим інструментом для формування необхідного балансу між потребою у вільному обміні інформацією і допустимими обмеженнями на її поширення.

Норми чинного законодавства відповідно є основою для гарантування фундаментальних демократичних цінностей, пов'язаних з правом кожного суб'єкта на інформацію та свободу інформаційної діяльності, а також встановлюють режим доступу до інформації в цілому і в процесі міжнародного інформаційного співробітництва зокрема.

Інформація за режимом доступу поділяється на відкриту інформацію та інформацію з обмеженим доступом, а остання в свою чергу — на конфіденційну і таємну. До таємної належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю⁷⁸. Правовий режим кожного виду інформації з обмеженим доступом (державної таємниці, інших передбачених законодавством таємниць та конфіденційної інформації) відрізняється один від одного змістом режиму доступу до носіїв зазначених відомостей. Його сутність полягає в установленні обмежень доступу до інформації, зокрема, стосовно державної таємниці — встановленням ступенів її секретності («особливої важливості», «цілком таємно», таємно»); щодо іншої інформації з обмеженим доступом — її конфіденційності. Ступінь секретності та конфіденційності — це категорії, які характеризують важливість інформації і визначають ступінь обмеження доступу до неї та рівень її охорони.

Режим доступу до інформації є важливою складовою її правового режиму, його основою. Ступінь секретності та конфіденційності та встановлені відповідно до них грифи секретності і конфіденційності на матеріальних носіях інформації диктують усім суб'єктам, діяльність яких пов'язана з нею, порядок поводження з такою інформацією.

В Україні на рівні актів законодавства зміст поняття «правовий режим інформації» залишається невизначеним, містяться тільки окремі фрагменти правового режиму конкретних видів

інформації з обмеженим доступом, що не становить державної таємниці. Лише Закон України «Про державну таємницю»⁷⁹ містить чітке визначення змісту поняття «державна таємниця», комплекс правових норм, котрі встановлюють правовий режим інформації, що становить державну таємницю, а саме: перелік інформації, що може бути віднесена до державної таємниці, порядок її віднесення до цієї категорії відомостей та їх засекречування; зміст режиму доступу до інформації, що становить державну таємницю та правових норм його забезпечення; основні організаційно-правові заходи щодо охорони державної таємниці, які відповідають встановленому рівню обмежень доступу до цієї інформації та її носіїв; здійснення права власності на секретну інформацію та її матеріальні носії, компетенцію суб'єктів України щодо встановлення правового режиму відомостей, віднесених до державної таємниці та його додержання; відповідальність суб'єктів держави за порушення вимог чинного законодавства про державну таємницю.

Важливим є те, що Закон України «Про державну таємницю» чітко визначає відомості, що не належать до державної таємниці та забороняє «віднесення до державної таємниці будь-яких відомостей, якщо цим будуть звужуватися зміст і обсяг конституційних прав та свобод людини і громадянина, завдаватиметься шкода здоров'ю та безпеці населення»⁸⁰. Тобто цей закон встановлює правовий режим відомостей, що містять державну таємницю, передбачає гарантії захисту прав і свобод людини, проголошених Конституцією України.

Правові норми регулювання суспільних інформаційних відносин щодо «інших передбачених законодавством таємниць та конфіденційної інформації» чинне законодавство не визначає. А деякі норми законів можуть тлумачитися неоднозначно або є незрозумілими за змістом.

Так, у ст. 30 Закону України «Про інформацію» встановлено, що «громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу... самостійно визначають режим доступу до неї, включаючи належність її до конфіденційної...». Зміст цієї правової норми свідчить про те, що така інформація може бути

як конфіденційною, так і іншою, передбаченою законом таємницею. Окрім того, незрозуміло, що включається до складу інформації «професійного, ділового, виробничого та іншого характеру». А також не може бути підставою (критерієм) для віднесення до категорії конфіденційної інформації наявності до неї «іншого інтересу», тому що такий інтерес може мати й кримінальну спрямованість.

Необхідність встановлення правового режиму кожного виду інформації з обмеженим доступом передбачена фактично і базовим для інформаційної сфери Законом України «Про інформацію»⁸¹, який передбачає:

- забезпечення законності одержання, використання, поширення та зберігання інформації (ст. 5);
- створення загальної системи охорони інформації (ст. 6);
- встановлення режиму доступу до інформації на підставі порядку, передбаченого правовими нормами (ст. 28);
- поділ інформації за режимом доступу на відкриту та з обмеженим доступом (ст. 28);
- віднесення інформації до категорії таємних відомостей, порядок і терміни обнародування таємної інформації тільки на підставі відповідних законів (ст. 30);
- регулювання законодавством права власності на інформацію (ст. 38) та охорони цього права законом (ст. 45);
- встановлення відповідальності за порушення законодавства про інформацію (ст. 47);
- гарантування інформаційного суверенітету України на підставі забезпечення виключного права власності України на інформаційні ресурси, що формуються за рахунок коштів державного бюджету, встановленням режиму доступу інших держав до цих ресурсів та використання їх на основі рівноправного співробітництва з іншими державами (ст. 53 — 54).

Наведене свідчить про те, що правові норми Закону України «Про інформацію» передбачають розвиток інформаційного законодавства на підставі впровадження на рівні законів правових норм удосконалення правового режиму різних видів інформації з обмеженим доступом.

У світлі наведеного розглянемо правовий режим науково-технічної інформації. Закон України «Про науково-технічну інформацію»⁸² визначає, що:

— науково-технічна інформація — це документовані або публічно оголошені відомості про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності;

— інформаційні ресурси науково-технічної інформації — це систематизоване зібрання науково-технічної літератури і документації (книги, брошури, періодичні видання, патентна документація, нормативно-технічна документація, промислові каталоги, конструкторська документація, звітна науково-технічна документація, депоновані рукописи, переклади науково-технічної літератури і документації), зафіксовані на паперових чи інших носіях.

Закон визначає правовий режим науково-технічної інформації (розд. II). Він закріплює право усіх громадян України, юридичних осіб, державних органів, органів місцевого і регіонального самоврядування відповідно до Конституції України і цього закону на відкриту науково-технічну інформацію, що передбачає можливість вільного її одержання, зберігання, використання і поширення під час здійснення наукової, науково-дослідної, виробничої, громадської та іншої діяльності, що не забороняється чинним законодавством. А також регламентує право власності на науково-технічну інформацію та відносини між власниками науково-технічної інформації, її споживачами і посередниками.

Законом «Про науково-технічну інформацію» встановлено, що режим доступу до відкритої науково-технічної інформації та інформації з обмеженим доступом регулюється чинним законодавством (ст. 5, п. 2). Окрім того, законом також встановлено порядок формування ринку науково-технічної інформації, умови надання інформаційної продукції та послуг на безоплатній і комерційній основі⁸³. При цьому норма закону визначає, що в ході здійснення купівлі-продажу інформаційної продукції мають гарантуватись охорона прав інтелектуальної власності, державної та комерційної таємниці, законні права та інтереси власника і виробника інформаційної продукції і послуг⁸⁴.

Закон України «Про науково-технічну інформацію» відповідно до міжнародних правових норм, світової практики та правових норм Конституції України⁸⁵ встановлює, що основу інфор-

маційної діяльності в сфері науково-технічної інформації становлять права і свободи, непорушність права власності на відповідну інформацію, що обмеження цих прав і свобод є винятком із загальних правил і встановлюється тільки законами.

Зміст поняття «режим доступу до інформації» визначено Законом України «Про інформацію». Це «передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації»⁸⁶. При цьому нагадаємо, що відповідно до законодавства за режимом доступу інформація поділяється на відкриту та з обмеженим доступом.

Відкрита інформація, тобто інформаційна продукція, та послуги на її основі надаються безоплатно або на комерційних умовах. Доступ до інформації з обмеженим доступом встановлюється правовими нормами, що включають порядок і правила обмеження доступу, основу яких становлять:

- порядок і правила віднесення інформації до категорії з обмеженим доступом та визначення ступеня її секретності або конфіденційності;

- порядок і правила засекречування, надання конфіденційності конкретній інформації з обмеженим доступом шляхом позначення носіїв такої інформації грифом секретності або конфіденційності, які відповідають встановленому ступеню її секретності або конфіденційності (ст. 4).

Таким чином, віднесення інформації до категорії з обмеженим доступом її засекречування або визначення конфіденційності слід розуміти як відокремлення таких відомостей із загальнодоступної інформації та встановлення обмежень до неї з метою запобігання негативним наслідкам для особи, суспільства, держави в разі їх витоку, розголошення або несанкціонованого використання.

Основою захисту інформації з обмеженим доступом є захист державної таємниці. Ця система створюється державою, в ній зосереджуються найкращі технології та найкращі і найбільш підготовлені кадри. Безумовно, високий рівень захисту державної таємниці є важливою передумовою для формування загальної системи захисту інформації з обмеженим доступом. Участь держави у формуванні системи захисту державної таємниці зумовила те, що віднесення відомостей до цієї категорії та їх

засекречування, всебічним і ґрунтовним в методологічному, правовому і організаційному планах як в Україні, так і за кордоном.

Зокрема, Законом України «Про державну таємницю» поняття «віднесення інформації до державної таємниці» визначено, як процедура прийняття (державним експертом з питань таємниці) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їх секретності шляхом обґрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю та з опублікуванням цього Зводу, змін до нього⁸⁷.

Законом України «Про державну таємницю» встановлено, що державний експерт з питань таємниць здійснює відповідно до вимог цього закону віднесення інформації у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, зміни ступеня цієї інформації та її розсекречування (ст. 9).

Закон чітко визначає повноваження державних експертів з питань таємниць, регламентує порядок віднесення інформації до державної таємниці, процедури прийняття рішення державним експертом та зміст цього рішення⁸⁸. При цьому слід нагадати, що в рішенні державного експерта з питань таємниць зазначаються:

- — інформація, яка має становити державну таємницю, та її відповідність категоріям і вимогам, передбаченим законом;

- підстави для віднесення інформації до державної таємниці та обґрунтування шкоди національній безпеці України у разі її розголошення;

- ступінь секретності цієї інформації;

- обсяг фінансування заходів, необхідних для її охорони;

- *- орган державної влади, місцевого самоврядування, підприємство, установа, організація чи громадянин, який вніс пропозицію про віднесення цієї інформації до державної таємниці, та орган державної влади (органи), якому надається право визначати коло суб'єктів, які матимуть доступ до цієї інформації;

- строк, протягом якого діє рішення про віднесення інформації до державної таємниці⁸⁹.

Законодавством також встановлена персональна відповідальність державного експерта з питань таємниць за законність і обґрунтованість свого рішення про віднесення інформації до державної таємниці або висновку про зниження ступеня секретності такої інформації чи скасування рішення про віднесення її до державної таємниці, а також за умисне неприйняття рішення про віднесення до державної таємниці інформації, розголошення якої може завдати шкоди інтересам національної безпеки України⁹⁰.

Рішення державного експерта з питань таємниць підлягає реєстрації спеціально уповноваженим органом державної влади у Зводі відомостей, що становлять державну таємницю (ЗВДТ), як це передбачено ст. 11 закону. Інформація вважається державною таємницею з часу опублікування ЗВДТ, до якого включена ця інформація, чи зміни до нього в порядку, встановленому законом⁹¹.

Рішенням державного експерта з питань таємниць можуть бути встановлені ступені секретності відомостей, віднесених до державної таємниці: «особливої важливості», «цілком таємно», «таємно».

Відповідно до чинного законодавства встановлено, що на підставі та в межах Зводу відомостей, що становлять державну таємницю, з метою конкретизації та систематизації даних про секретну інформацію органи державної влади створюють галузеві або відомчі розгорнуті переліки відомостей, що становлять державну таємницю, а також можуть створювати міжгалузеві або міжвідомчі розгорнуті переліки відомостей, що становлять державну таємницю. Підприємства, установи та організації, незалежно від форм власності, що провадять діяльність, пов'язану з державною таємницею, за ініціативою та погодженням із замовником робіт, пов'язаних з державною таємницею, можуть створювати власні розгорнуті переліки відомостей, що становлять державну таємницю. Розгорнуті переліки, розроблені на підставі ЗВДТ, погоджуються із спеціально уповноваженим органом державної влади у сфері охорони державної таємниці, затверджуються державним експертом з питань таємниць та реєструються у спеціально уповноваженому органі державної влади⁹².

Таким чином, в організаційному і правовому плані чинне законодавство України чітко визначає порядок і правила віднесення відомостей до державної таємниці, компетенцію державних експертів з питань таємниць щодо вирішення цих питань, порядок набуття чинності рішень (висновків) державних експертів та їх відповідальність за законність і обґрунтованість прийнятих рішень (висновків). Тобто процедура віднесення відомостей до державної таємниці, компетенцію державних експертів з питань таємниць щодо вирішення цих питань, порядок набуття чинності рішень (висновків) державних експертів та їх відповідальність за законність і обґрунтованість прийнятих рішень (висновків). Тобто процедура віднесення відомостей до державної таємниці персоніфікується, що дає змогу стосовно будь-якої інформації, віднесеної до державної таємниці, встановити мотивацію цього та державного експерта, яким прийнято це рішення. Крім того, формування на основі рішень державних експертів з питань таємниць ЗВДТ та в його межах — розгорнутих переліків відомостей, що становлять державну таємницю, створює умови для здійснення єдиної державної політики щодо встановлення обмежень доступу до такої інформації (визначення ступенів секретності і засекречування) та забезпечення відповідного рівня її охорони.

Система віднесення відомостей до державної таємниці та її засекречування, відповідно до встановлених ступенів секретності, впроваджена в Україні з урахуванням досвіду інших країн.

Зокрема, у світовій практиці діють такі системи віднесення інформації до державної таємниці та її засекречування, як:

- перелікова система;
- система первинного і похідного віднесення відомостей до державної таємниці та її засекречування;
- система програмно-цільового підходу;
- змішана система.

У США діє система первинного і похідного віднесення відомостей до державної таємниці та їх засекречування. Сутність цієї системи полягає у: визначенні законодавцем категорії інформації, що підлягає віднесенню до державної таємниці⁹³; надання Президентом повноважень посадовим особам, які здійснюють первинне засекречування цієї інформації⁹⁴; здійсненні уповноваженими посадовими особами похідного засекречуван-

ня інформації на підставі змісту первинних секретних відомостей⁹⁵.

У Російській Федерації віднесення відомостей до державної таємниці та їх засекречування містить елементи первинної і перелікової систем. Законом визначаються відомості, котрі можуть бути віднесені до державної таємниці⁸⁶, Президентом РФ затверджується перелік посадових осіб, яким надаються повноваження щодо віднесення відомостей до державної таємниці. На підставі рішень вказаних посадових осіб формується Перелік відомостей, віднесених до державної таємниці. Цей перелік є підставою для надання документам та іншим носіям інформації відповідного грифу секретності, відповідного ступеня секретності інформації, визначеного у цьому переліку⁹⁷.

В Україні діє первинно-перелікова система з елементами програмно-цільового підходу щодо віднесення відомостей до державної таємниці та їх засекречування. Первинно інформація, що може бути віднесена до державної таємниці і підлягає засекречуванню, визначається законодавцем у сферах: оборони, економіки, науки і техніки; зовнішніх відносин; державної безпеки та охорони правопорядку⁹⁸. На підставі рішень державних експертів з питань таємниць формується Звід відомостей, що становлять державну таємницю, в межах і на підставі якого створюються розгорнуті переліки відомостей. Окрім того, законом встановлено, що ступені секретності науково-дослідних, дослідно-конструкторських і проектних робіт, які виконуються в інтересах забезпечення національної безпеки та оборони держави, встановлюються державним експертом з питань таємниць, який виконує свої функції в сфері діяльності замовника, разом з підрядником⁹⁹. А це вже елементи програмно-цільового підходу до віднесення відомостей до державної таємниці та їх засекречування. Сутність цього підходу полягає в тому, що державний експерт, виходячи з вимог ЗВДТ та відповідного розгорнутого переліку відомостей, віднесених до державної таємниці, визначає ступені секретності цілей та результатів досліджень і розробок з встановленням строків дії обмежень доступу до них. Тобто програмно-цільовий підхід передбачає віднесення до державної таємниці відомостей про заплановані перспективні результати (проміжні і остаточні) науково-дослідних, дослідно-конструкторських і проектних робіт.

Відомостям, віднесеним до державної таємниці, надається відповідний ступінь секретності. Як свідчить світова практика, кожна держава визначає і певні критерії для встановлення відповідного ступеня секретності.

Наприклад, у США встановлені такі ступені секретності відомостей, віднесених до державної таємниці та критерії їх визначення, як:

- цілком таємно — надається інформації, несанкціоноване розкриття якої може завдати надзвичайно серйозної шкоди національній безпеці;

- таємно — надається інформації, несанкціоноване розкриття якої може завдати серйозної шкоди національній безпеці;

- конфіденційно — надається інформації, несанкціоноване розкриття якої може завдати шкоди національній безпеці¹⁰⁰.

У Російській Федерації встановлені три ступені секретності відомостей, віднесених до державної таємниці, і відповідно до цих ступенів грифи секретності для носіїв такої інформації — «особливої важливості», «цілком таємно», «таємно»¹⁰¹. Критерії віднесення відомостей до державної таємниці встановлені підзаконним актом відповідно до ступенів секретності:

- особливої важливості — відомості в галузі військової, зовнішньополітичної, економічної, науково-технічної, розвідувальної, контррозвідувальної та оперативно-розшукової діяльності, поширення яких може завдати шкоди інтересам Російської Федерації в одній або кількох із перелічених галузей;

- цілком таємно — відомості в галузі військової, зовнішньополітичної, економічної, науково-технічної, розвідувальної, контррозвідувальної та оперативно-розшукової діяльності, поширення яких може завдати шкоди інтересам міністерства (відомства) або галузі економіки Російської Федерації в одній або кількох із перерахованих галузей;

- таємно — усі інші відомості, що становлять державну таємницю, поширення яких може завдати шкоди інтересам підприємства, установи чи організації в перелічених вище сферах діяльності.

І в США, і в Російській Федерації відмінність між ступенями секретності відомостей, віднесених до державних таємниць, зумовлена розміром шкоди інтересам:

— у США — «надзвичайно серйозної», «серйозної», просто «шкоди» національній безпеці;

— у Російській Федерації — інтересам держави в одній або кількох галузях; інтересам міністерства (відомства) в одній або кількох галузях; інтересам підприємства, установи, організації.

Підходи до віднесення відомостей до державних таємниць у США і Російській Федерації та засекречування цих відомостей створюють передумови для суб'єктивізму в процесі вирішення цих питань¹⁰². На думку автора, це пов'язано з тим, що поняття, види і розмір шкоди розроблені поки що недостатньо і будуть відрізнятися для кожного конкретного об'єкта захисту, виходячи із змісту відомостей, що становлять державну таємницю, сутності відображених у ній фактів, подій, явищ дійсності.

Українську систему віднесення відомостей до державної таємниці та визначення ступеня їх секретності слід вважати більш ґрунтовною. Процедури і правила вирішення цих питань встановлюються «Методичними рекомендаціями державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності» (далі — «Методичні рекомендації»), остаточна редакція яких введена в дію в лютому 1998 року¹⁰³. Підставою для віднесення відомостей до державної таємниці є сукупна шкода, що може бути завдана державі внаслідок розголошення конкретних відомостей, яка включає економічну шкоду та інші тяжкі наслідки, сутність яких полягає в такому:

— економічна шкода — матеріальні збитки державі у сферах оборони, економіки, зовнішніх відносин, державної безпеки і охорони правопорядку в кількісному вираженні, які спричинені чи можуть бути спричинені внаслідок розголошення конкретних відомостей, що становлять державну таємницю;

— інші тяжкі наслідки — негативні зміни у зазначених сферах (головним чином у сферах зовнішніх відносин, державної безпеки і охорони правопорядку), які відбулися чи можуть відбутися внаслідок розголошення конкретних відомостей, що становлять державну таємницю і які не піддаються економічному обрахунку в кількісному (вартісному) вираженні¹⁰⁴.

«Методичні рекомендації» встановлюють, що розмір економічної шкоди та тяжкості інших негативних наслідків визначаються за принципом експертних оцінок у однакових умовних

одиницях (балах), які є критеріями визначення ступеня секретності відомостей, а саме:

— від 1 до 10 балів — для відомостей зі ступенів секретності «таємно»;

— від 10 до 100 балів — для відомостей зі ступенями секретності «цілком таємно»;

— 100 балів і більше — для відомостей зі ступенями секретності «особливої важливості».

Таким чином, віднесення інформації до державної таємниці у сфері науки здійснюється за загальним порядком і правилами, встановленими чинним законодавством, відповідно до первинно-перелікової системи. А стосовно науково-дослідних, дослідно-конструкторських і проектних робіт, які виконуються в інтересах національної безпеки та оборони держави застосовується програмно-цільовий підхід. Тобто державний експерт з питань таємниць, який виконує функції у сфері діяльності замовника, разом з підрядником приймає рішення про віднесення до державної таємниці відомостей про заплановані проміжні й остаточні результати цих робіт.

Правові механізми регулювання відносин, пов'язаних із віднесенням інформації до державної таємниці про об'єкти промислової власності, визначено Положенням про порядок оформлення і використання прав на винаходи, корисні моделі і промислові зразки, що становлять державну таємницю, затвердженим постановою Верховної Ради України від 19 січня 1995 року. Цей нормативний документ встановлює: «Якщо об'єкт промислової власності створено з використанням інформації, зареєстрованої у Зводі відомостей, що становлять державну таємницю, то громадянин або юридична особа, яка є заявником, подає через режимно-секретний орган у Департамент України заявку, в якій містяться пропозиції про віднесення об'єкта промислової власності до державної таємниці»¹⁰⁵. Державне патентне відомство визначає державного експерта (експертів) з питань таємниць, до компетенції якого належить розгляд питання про цей об'єкт промислової власності та надсилає йому комплект матеріалів заявки для прийняття рішення про віднесення об'єкта промислової власності до державної таємниці.

На розгляд цього питання державному експерту з питань таємниць встановлено строк до двох місяців¹⁰⁶. Прийняте рішення

ня, відповідно до встановленого порядку, не пізніше як через десять днів з моменту його підписання надсилається для реєстрації до спеціально уповноваженого органу у сфері охорони державної таємниці. Окрім того, державний експерт з питань таємниць у своєму рішенні визначає державні органи, до відання яких переходить інформація, віднесена до державної таємниці, якому надається право приймати рішення щодо кола підприємств, установ і організацій, що матимуть доступ до секретного об'єкта промислової власності. Визначений державний орган здійснює повноваження щодо обмеження доступу до цього об'єкта промислової власності протягом чинності рішення державного експерта з питань таємниць¹⁰⁷.

Положенням про порядок оформлення і використання прав на винаходи, корисні моделі і промислові зразки, що становлять державну таємницю, визначено, що розгляд питань про зміни встановленого ступеня секретності об'єкта промислової власності переглядається відповідним державним експертом з питань таємниць не рідше, ніж один раз на три роки. За клопотанням заявника такий перегляд може здійснюватися частіше, однак не більш як один раз протягом року¹⁰⁸.

Чинним законодавством визначено, що строк, протягом якого діє рішення про віднесення інформації до державної таємниці, встановлюється державним експертом з питань таємниць з урахуванням ступеня секретності інформації, що він не може перевищувати для інформації зі ступенем секретності «особливої важливості» — 30 років, для інформації «цілком таємно» — 10 років, для інформації «таємно» — 5 років. Окрім того, Президент України з власної ініціативи або на підставі пропозицій державних експертів з питань таємниць чи за зверненням органів державної влади, місцевого самоврядування, підприємств, установ, організацій або громадян може встановлювати триваліші строки дії рішень про віднесення інформації до державної таємниці, ніж передбачені законом. Після закінчення передбаченого законом строку дії рішення про віднесення інформації до державної таємниці державний експерт з питань таємниць робить висновок про скасування рішення про віднесення її до державної таємниці або приймає рішення про продовження строку дії зазначеного рішення в межах строків, встановлених законодавством¹⁰⁹.

І ще один важливий аспект щодо віднесення інформації до державної таємниці.

Підвищення або зниження ступеня секретності інформації та скасування рішення про віднесення її до державної таємниці здійснюється на підставі висновку державного експерта з питань таємниць або рішення суду у випадках, передбачених законом, та внесення відповідних змін до Зводу відомостей, що становлять державну таємницю¹¹⁰.

Судове рішення з цих питань, як визначено законом, може бути прийняте на підставі оскарження заінтересованими громадянами включення до Зводу відомостей, що становлять державну таємницю, або до розглянутих переліків цих відомостей інформації, яка не відповідає категоріям і вимогам, передбаченим законом, або порушення встановленого порядку віднесення інформації до державної таємниці¹¹¹.

Інформація вважається державною таємницею з більш високим чи нижчим ступенем секретності або такою, що не становить державної таємниці, з часу опублікування змін до Зводу відомостей, що становлять державну таємницю¹¹².

Нагадаємо, що відповідно до Закону України «Про державну таємницю» ступінь секретності («особливої важливості», «цілком таємно», «таємно» — це категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою¹¹³.

У сфері, пов'язаній з інформацією з обмеженим доступом, що не становить державної таємниці, доцільно розглядати таку категорію, як конфіденційність інформації, що характеризує важливість інформації, ступінь обмеження доступу до неї та рівень її охорони: стосовно такої інформації, що є власністю держави, — з боку держави; конфіденційної інформації, що є приватною власністю, — з боку її власника. При цьому слід врахувати, що режим доступу до будь-якої інформації встановлюється правовими нормами національного законодавства. Тобто як держава, так і власник приватної інформації, встановлюючи обмеження на її поширення, зобов'язані діяти в межах правового поля держави.

Засекречування матеріальних носіїв інформації здійснюється шляхом надання відповідному документу, виробу або іншому матеріальному носію інформації грифу секретності. Законом

встановлено, що гриф секретності — це реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності цієї інформації¹¹⁴.

Реквізити кожного матеріального носія секретної інформації мають містити гриф секретності, який відповідає ступеню секретності інформації, встановленому рішенням державного експерта з питань таємниць, — «особливої важливості», «цілком таємно», «таємно», дату та строк засекречування матеріального носія секретної інформації, що встановлюється з урахуванням передбачених законом строків дії рішення про віднесення інформації до державної таємниці, підпис, посаду особи, яка надала зазначений гриф, а також посилання на відповідний пункт (статтю) Зводу відомостей, що становлять державну таємницю¹¹⁵. Тобто як у системі віднесення відомостей до державної таємниці, так і їх засекречування, вирішення цих питань персоналізується. А це дає змогу встановити персональну відповідальність за правомірність віднесення відомостей до державної таємниці та за їх засекречування.

Відповідно до закону «перелік посад, які дають право посадовим особам, що їх займають, надавати матеріальним носіям секретної інформації грифи секретності, затверджується керівником органу державної влади, органу місцевого самоврядування підприємства, установи, організації, що провадить діяльність, пов'язану з державною таємницею»¹¹⁶. Чинне законодавство також визначає, що строк засекречування матеріальних носіїв інформації має відповідати строку дії рішення про віднесення інформації до державної таємниці, встановленого рішенням державного експерта з питань таємниць, що перебіг строку засекречування матеріальних носіїв інформації починається з часу надання їм грифу секретності¹¹⁷.

Загальні правила і порядок засекречування інформації, визначені чинним законодавством, поширюються на всі види діяльності, пов'язані з державною таємницею. Однак доцільно враховувати деякі особливості засекречування у сфері наукової діяльності.

Відповідно до ступеня секретності науково-дослідних, дослідно-конструкторських і проектних робіт, які виконуються в інтересах забезпечення національної безпеки і оборони держави, встановлені державним експертом з питань таємниць, здійсню-

ється засекречування цих робіт. Вирішення цих питань згідно із нормативними вимогами покладається на замовника разом з підрядником. Механізм цього має бути таким. Посадові особи замовника таких робіт разом з посадовими особами підрядника, які в установленому порядку мають право надавати матеріальним носіям секретної інформації грифи секретності, у завданнях (технічні, тактико-технічні завдання) на використання досліджень і розробок визначають такі грифи секретності:

- дослідження, розробки (НДДКР) проектної роботи в цілому;
- конкретних етапів робіт, отриманих проміжних і кінцевих результатів;
- звітної і конструкторсько-технологічної документації в цілому або їх окремих частин.

Можуть також засекречуватися цілі досліджень і розробок, а також зовнішній вигляд дослідних (експериментальних) зразків за умов, якщо це передбачено рішенням державного експерта з питань таємниць.

Таким чином, законодавство визначає лише основні вимоги щодо порядку віднесення відомостей у сфері науки до державної таємниці та їх засекречування. Для реалізації цих вимог законодавства доцільне вдосконалення правових механізмів вирішення проблем засекречування в науці, особливо стосовно фундаментальних досліджень у зв'язку з великою невизначеністю їх кінцевих результатів, багатофункціональністю і багато-варіантністю практичного застосування.

Незважаючи на те, що наприкінці минулого століття геополітична ситуація змінилася, деякі загрози національній безпеці зникли, з'явилися нові, не менш небезпечні. А це передбачає і певну орієнтацію фундаментальних і прикладних досліджень з реалізацією вираженої державної політики засекречування їх результатів. Правові механізми вирішення цих питань поки що недосконалі. Для цього передусім доцільно подолати існуючі в Україні дві тенденції, а саме: перша — максимальне засекречування як метод збереження для держави унікальних наукових здобутків; друга — наука має бути відкритою і не повинна засекречуватися. Перша тенденція виходить за межі розумної закритості; друга — за межі розумної відкритості. Тому потрібен

посередник у вигляді ефективно діючого правового механізму та відповідних організаційних заходів держави.

Загальний гриф секретності завдання (технічного, тактико-технічного завдання) на виконання науково-дослідних, дослідно-конструкторських робіт має відповідати найвищому грифу секретності цих робіт, що відповідає ступеню їх секретності, встановленому державним експертом з питань таємниць. У процесі виконання досліджень і розробок найвищий гриф секретності відповідно до встановленої державним експертом ступінь секретності надається документації, виробам лише в тій частині, яка відповідає цьому ступеню секретності.

Засекречування науково-дослідних, дослідно-конструкторських і проектних робіт (етапів, результатів, документації, виробів) у процесі їх виконання зобов'язані здійснювати посадові особи підприємця, які в установленому порядку отримали право надавати матеріальним носіям секретної інформації грифи секретності. Державний експерт з питань таємниць, замовник досліджень і розробок, державний орган, до сфери управління якого належить підприємця та спеціально уповноважений державний орган у сфері охорони державної таємниці, в установленому законодавством порядку здійснюють контроль за дотриманням порядку і правил засекречування науково-дослідних, дослідно-конструкторських і проектних робіт у процесі їх виконання.

Певні особливості має і засекречування об'єктів промислової власності, що впливають із вимог Положення про порядок оформлення і використання прав на винаходи, корисні моделі і промислові зразки, що становлять державну таємницю¹¹⁸.

Цей нормативно-правовий документ розглядає два аспекти створення об'єктів промислової власності, а саме:

- перший, за умов, за яких об'єкт промислової власності створено з використанням інформації, зареєстрованої у Зводі відомостей, що становлять державну таємницю;

- другий, якщо об'єкт промислової власності створено з використанням інформації, яка відповідно до ст.8 Закону України «Про державну таємницю» може бути віднесена до державної таємниці.

В обох наведених випадках автори об'єктів промислової власності мають поводитися з матеріалами на ці об'єкти як з таки-

ми, що містять державну таємницю. Заявки на винаходи, корисні моделі і промислові зразки з пропозиціями про віднесення їх до державної таємниці до державного потенційного відомства надсилаються через режимно-секретний орган заявника. Якщо матеріали на об'єкт промислової власності, що пропонується віднести до державної таємниці, неможливо надіслати патентному відомству через режимно-секретний орган заявника, це питання вирішується через режимно-секретний орган місцевого органу державної виконавчої влади за місцем розташування (для юридичних осіб), за місцем мешкання (для фізичних осіб)¹¹⁹.

Рішення державного експерта про віднесення об'єкта промислової власності до державної таємниці, прийняте на підставі подання державного патентного відомства, реєструється в спеціально уповноваженому державному органі з питань охорони державної таємниці.

Винахід, корисна модель, промисловий зразок вважаються секретними об'єктами промислової власності і підлягають засекречуванню з наданням відповідних реквізитів, передбачених ст.15 Закону України «Про державну таємницю» за умов, що державним патентним відомством експертиза проведена по суті, а саме:

- у випадку, якщо об'єкт промислової власності створено з використанням відомостей, зареєстрованих у Зводі відомостей, що становлять державну таємницю, з моменту прийняття рішення державним експертом з питань таємниць про віднесення цього об'єкта промислової власності до державної таємниці;

- у випадках, якщо об'єкт промислової власності створено з використанням відомостей, що можуть бути віднесені до державної таємниці відповідно до ст.8 Закону України «Про державну таємницю», з моменту опублікування відповідних доповнень до Зводу відомостей, які становлять державну таємницю.

Строк дії документа, що засвідчує право авторства на експертний об'єкт промислової власності, встановлюється на строк засекречування об'єкта промислової власності, однак не більше строку дії патенту на відповідний об'єкт промислової власності, який встановлюється законодавством України з питань охорони промислової власності.

Відповідно до ступеня секретності інформації та грифів секретності матеріальних носіїв такої інформації відповідно до світової практики встановлюються єдині вимоги до виготовлення, обліку, користування, зберігання схоронності, передачі та транспортування секретних матеріальних носіїв інформації. Тобто ступінь секретності інформації та відповідний йому гриф секретності диктують усім суб'єктам порядок поводження з матеріальними носіями інформації з обмеженим доступом. Законом встановлено, що вимоги стосовно поводження із засекреченою інформацією та її матеріальними носіями встановлюються Кабінетом Міністрів України¹²⁰.

У процесі міжнародного співробітництва інформація, що містить державну таємницю, одержана від інших держав, засекречується відповідно до вимог національного законодавства. Тобто обмеження доступу до такої інформації встановлюється відповідно до узгоджених ступенів секретності носіїв інформації, що передається (отримується) сторонами в процесі такого співробітництва. Закон України «Про державну таємницю» цей порядок регламентує так: «Передані Україні відомості, що становлять таємницю іноземної держави чи міжнародної організації, охороняються в порядку, передбаченому цим Законом. У разі, якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, встановлено інші, ніж передбачені цим Законом, правила охорони таємниці іноземної держави чи міжнародної організації, то застосовуються правила міжнародного договору України»¹²¹. А це передбачає у випадках, якщо національні законодавства сторін містять різні вимоги до порядку обмеження доступу до інформації, що охороняється відповідно до світової практики і нормативних вимог, чинних в Україні, взаємно узгодженні критерії і правила у вигляді зобов'язань сторін викладаються у відповідній угоді (договорі). Наведені вимоги є обов'язковими і в процесі міжнародного співробітництва щодо наукової та науково-технічної діяльності з використанням інформації, що становить державну таємницю.

Таким чином, обмеження доступу до науково-технічної інформації (інформативних ресурсів науково-технічної інформації), тобто віднесення її до інформації з обмеженим доступом,

здійснюється відповідно до правового режиму інформації та його складової — режиму доступу до відповідного виду інформації. Загальновизначеним у світовій практиці є принцип відкритості інформації, дотримання права на інформацію і свободи інформаційної діяльності та гарантування права власності на інформацію. Обмеження доступу до інформації (віднесення до категорії з обмеженим доступом, засекречування, встановлення її конфіденційності) є винятком із загального принципу відкритості інформації і здійснюється тільки на основі законодавства.

Віднесення інформації до категорії з обмеженим доступом, її засекречування, надання конфіденційності в науці здійснюється з мотивів забезпечення прогресивного розвитку економіки, підвищення конкурентоспроможності національних товарів на світовому ринку та в інтересах національної безпеки будь-якої країни.

Встановлення обмежень до науково-технічної інформації (інформаційних ресурсів науково-технічної інформації), віднесеної до державної таємниці, дає змогу діяти переважно в межах правового поля держави. Стосовно іншої інформації з обмеженим доступом, що не становить державної таємниці у зв'язку з фрагментарним визначенням її правового режиму, розв'язання проблем обмеження доступу до неї відповідно до визначених у світі стандартів є проблематичним.

Створення будь-якої сучасної військової техніки й озброєння базується на фундаментальній науці, яка займається вивченням явищ природи і суспільства як таких. Об'єктом фундаментальних науково-дослідних робіт є експериментальні або теоретичні роботи, спрямовані на одержання нових знань, вони мають багатофункціональну спрямованість, іноді без конкретної мети. Закономірності й властивості явищ, які досліджуються, зумовлюють розвиток багатьох прикладних досліджень у різних галузях науки і лише деяка частина нових знань безпосередньо використовується.

Інформаційні ресурси лише тоді мають цінність, коли вони є повними, автентичними, доступними, актуальними, проте в даний час в Україні це ще далеко не так. Існуючі відомчі й міжвідомчі інформаційні архівні, бібліотечні, державної статистики та інші системи, в яких, головним чином, і зосереджені

відкриті державні інформаційні ресурси (ВДІР), далекі від необхідної повноти, діють неузгоджено і, почасти, дублюють одна одну.

За офіційними статистичними даними, в Україні функціонує 1031 обчислювальний центр, де працює 116 тисяч фахівців у галузі інформатизації (дані на 1 січня 2000 рік), які володіють у цілому досвідом зі створення і використання автоматизованих інформаційних систем. На жаль, ні обсяг, ні якість інформаційного ресурсу, ні реалізовані технології для широкого використання цього ресурсу не дають підстав стверджувати, що він забезпечить ефективне інформаційне обслуговування суспільства. Тому введення ВДІР у господарський обіг на основі захищених інформаційних технологій займе не один рік, але перші кроки вже робити час. Таким кроком може стати створення Переліку основних заходів щодо забезпечення відкритості державних інформаційних ресурсів.

1.4.6. Особливості організації змістовного інформаційного ресурсу за науково-технічним доробком як об'єкта державного управління

З огляду на проблему державницького інтегрального підходу до управління інформацією інформаційні ресурси мають бути віднесеними до найважливіших стратегічних ресурсів держави, значення і вплив яких можна порівняти з впливом капіталу і праці в індустріальну епоху. Історичний досвід свідчить, що втрата державою і суспільством контролю над природним середовищем (ресурсами надр і науково-промисловою інфраструктурою) вело до втрати темпів розвитку і навіть державності. Сьогодні інформаційний ресурс України, наприклад у науково-технічній сфері, можна вважати стратегічним лише умовно, оскільки:

- не існує органу державної влади з функціями розробки та впровадження нормативних, методологічних, організаційно-фінансових заходів забезпечення реалізації державної політики у цій сфері діяльності;

- міністерства, інші державні органи створюють свої окремі інформаційні бази навіть без узгодження технологій їх формування;

- невизначеними досі є порядок і система огляду та поширення інформаційних ресурсів, які отримує Україна в процесі міжнародної діяльності, а також ресурсів, які містять відомості, віднесені до інформації з обмеженим доступом, хоча порядок її реєстрації та зберігання визначені окремими урядовими постановами;

- не сформовано системи інформаційного забезпечення участі вітчизняних науковців у міжнародних науково-технічних проектах, дослідженнях, розробках.

Це заважає Україні перейти від статусу країни-донора інтелектуального потенціалу до рівноправного науково-технічного співробітництва, сформувати систему державної реєстрації, накопичення та обігу інформаційних ресурсів не тільки у сфері науки і техніки, а й у сфері економіки, соціології, промислового і державного управління, забезпечити ними зацікавлені державні органи, наукові й освітні установи для підготовки аналітичних матеріалів, необхідних для прийняття державними органами місцевого і регіонального самоврядування рішень з питань науково-технічного, економічного і соціального розвитку з дотриманням обмежень, які передбачені світовими нормами і законодавством.

Зокрема, тлумачення і правила використання в Україні інформації, яка є предметом професійного, ділового, виробничого, банківського, комерційного інтересу громадян та юридичних осіб і не порушує передбачених законом таємниць, достатньо не опрацьовані.

За таких умов свобода інформаційної діяльності з додержанням визначених на рівні законів вимог режиму конфіденційності ділових інформаційних відносин значною мірою є показником громадської і професійної культури громадян — державних службовців, науковців, підприємців, спеціалістів — усіх учасників інформаційних відносин, оскільки інформаційні ресурси суспільства створюються інтелектуальною творчою працею людини. Крім того, слід врахувати, що інтелектуальна творчість визнає за талановитими людьми право піддавати сумніву будь-який науковий постулат, висловлюватися, вносити пропозиції щодо визнання норм існуючих обмежень свободи, тобто функцією вчених і фахівців є аналіз наявних наукових знань, засобів дій і

мислення, переоцінки правил, установлень, визнаних, існуючих у товаристві порядків і цінностей.

Усвідомлення системних, сутнісних, змістовних характеристик інформаційних процесів у ході прогресивного економічного і соціального розвитку, шляхів формування і розвитку національного інформаційного простору на основі об'єктивної, достовірної і соціально важливої інформації потребує фундаментальних досліджень взаємозв'язків «людина — природа — соціальна система — інформація».

Сьогодні влада України дедалі більше вирішує питань власності, розподілу і контролю над інформацією, усвідомлюючи, що застосування цього стратегічного ресурсу має не тільки фізичні наслідки (матеріальні ресурси, персонал, фінанси), а й впливає на людські переконання і стосунки.

Стан інформації України на сучасному етапі багато в чому визначається процесами реформування державних і суспільних структур, пов'язаними з переходом до відкритого, ринкового, соціально-орієнтованого суспільства. При цьому свою роль відіграють такі фактори, як різний рівень розвитку регіональних соціумів, перерозподіл відповідальності між центром і регіонами, серйозне відставання порівняно з передовими країнами в розробці та виробництві обчислювальної й телекомунікаційної техніки, використання новітніх інформаційних технологій і як наслідок — необхідність величезних інвестицій у інформатизацію.

В Україні постійно відбувається перерозподіл ресурсів, знань, досвіду. Державні органи НТІ все більше займаються інформаційною діяльністю на комерційній основі, диверсифікують свої зусилля в різних галузях інформатики, маркетингу, патентно-ліцензійної діяльності. У свою чергу підприємницький сектор бере активну, але неконтрольовану і некоординовану участь у формуванні державних змістовних ресурсів НТІ. Постає необхідність поєднати зусилля державного та комерційного секторів господарювання на функціональній основі¹²². При здійсненні такої політики необхідно враховувати, що державні інформаційні органи, які не отримують спеціального статусу від уряду, з неминучістю стають комерційними за суттю і державними за формою (внаслідок заборони їх приватизації). Це спричиняє до фінансових і професійних зловживань. Зауважимо, що для

структури комерційного сектору це не є характерним, окрім надзвичайних випадків, оскільки вони вирішують інформаційні завдання, що стоять перед ними, за рахунок власних коштів і ресурсів.

Сьогодні вплив держави на комерційний сектор здійснюється шляхом використання непрямих методів регулювання (на відміну від управління в державному секторі) через стандартизацію, сертифікацію інформаційної продукції, цінову та податкову політику, залучення комерційних інформаційних структур до участі в державних науково-технічних програмах.

Наявність різноманітних форм власності потребує вивчення нових організаційно-економічних форм діяльності організацій та служб, їх взаємодії, а також взаємодії із органами державної влади та управління та споживачами інформації. Важливими питаннями є подальша розробка принципів та методів формування ринку ШП, інформаційного маркетингу, проведення прогностичних досліджень розвитку інформаційного ринку в Україні, розробка економічних показників та нормативів діяльності державних органів НТІ, вдосконалення фінансово-господарського механізму науково-інформаційної діяльності, тобто всіх процесів, які є основою для здійснення управління СНІР.

Усі головні правові положення про національну систему НТІ, її державний та підприємницький сектори, закладені в Законі України «Про науково-технічну інформацію», але, на жаль, вони не набули подальшого розвитку.

З урахуванням законодавчих норм щодо змістовності інформації та її наукової і технічної вагомості в найбільш узагальненому вигляді інформаційний ресурс держави за результатами науково-технічної діяльності може бути визначений як сукупний продукт інтелектуальної діяльності професійно та творчо активної частини суспільства, який зафіксований на матеріальних носіях і може бути наданим у матеріальному або інформаційному вигляді, тобто розглядатися як інтелектуальна власність (ІВ).

Закон США «Про експортний контроль» (у ред. 1989 року, ст. 16, § 4) надає тлумачення матеріального як кінцевої науково-технічної продукції прикладних або теоретичних досліджень і визначається терміном «технологія»: «Інформація про «ноу-хау» (у вигляді моделі, прототипу, креслення, схем, діаграм,

навчання або технічних послуг), які можуть бути використані для проектування, виготовлення, виробництва, експлуатації або ремонту виробів, у тому числі програмне забезпечення ЕОМ, та технічні дані, але не самі вироби».

Простий опис об'єктів, методології (застосування), технології виробництва або його удосконалення слід розглядати як інформаційний вигляд ресурсу.

Розглядаючи проблеми інформаційного ринку, варто відразу зауважити, що інформація — категорія нематеріальна. Необґрунтований підхід до інформації як до товару приводить до неправильного розуміння її самої.

Інформаційні продукти і послуги є корисними результатами людської праці, що існують у матеріалізованих (видання, бази даних, роздруківки, екрани) і нематеріалізованих (усне інформування, інформаційний пошук за дорученням клієнта і т. п.) формах, хоча класична політична економія взагалі не розглядає інформацію та інформаційні продукти і послуги як товар, а тільки як нематеріальну категорію, однак право на використання набуває товарної форми й у цій формі виступає на ринку поруч із звичайними товарами.

Щодо визначення поняття «інформаційний ринок» є різні підходи. Власне, категорія «ринок» може бути визначена як «сфера товарного обігу, де формується попит, пропозиція і ціна на товари; визначене місце, де відбувається торгівля». «Інформаційний ринок» є частиною ринку, де предметом є специфічний товар — інформація, точніше, інформаційні продукти і послуги.

Інформаційний сектор економіки США почав формуватися у 50-х роках ХХ століття і в 70-х роках становив 46% валового національного продукту країни¹²³, а сьогодні жодна галузь промисловості сфери послуг вже не може ігнорувати його значення, оскільки індустрія переробки інформації включає обчислювальну техніку, зв'язок і телекомунікації, виробництво інформаційних продуктів і послуг. Уже в 1985 — 87 роках темпи зростання ринку інформаційних продуктів і послуг промислово розвинутих капіталістичних країн почали випереджати темпи зростання товарної продукції й експорту грошового капіталу, а середньорічні темпи зростання обсягів продажу на інформаційному ринку становили 16 — 25%¹²⁴. Інформаційні ресурси стали

набувати стратегічного значення. Великі промислові компанії стають одночасно і лідерами на ринку інформаційних продуктів і послуг, вважаючи, що використання інформаційних технологій — один із найбільш ефективних засобів підвищення конкурентоспроможності.

Сьогодні інформаційні продукти і послуги підпорядковуються законам товарного виробництва і ринку й мають виражену товарну природу. Їх можна визначити за секторами:

- ділової інформації, що охоплює біржову і фінансову, економічну і статистичну, комерційну інформацію та ділові новини;

- науково-фахової інформації: науково-технічної, медичної, юридичної й ін., що охоплює документальну, бібліографічну, реферативну, довідкову інформацію і дані в галузі фундаментальних і прикладних, природних, технічних і суспільних наук, галузей виробництва і сфер людської діяльності. Саме в цьому секторі передбачена організація доступу до першоджерел через систему поширення інформації, що включає спеціалізовані служби, бібліотечний сервіс і ін.;

- масової, споживчої інформації, що охоплює новини і літературу, довідники, енциклопедії, споживчу і розважальну інформацію, орієнтовану на домашнє, а не службове і промислове використання;

- соціально-політичної інформації, спрямований на обслуговування державної влади й управління статистичною, соціальною, архівною і спеціальною інформацією.

Сьогодні в Україні досить ефективно функціонують сектори масової інформації, інформації для спеціалістів, включаючи науково-технічну інформацію, де зосереджено приблизно 15 — 20% інформації, але саме його стан повною мірою визначає ступінь розвитку науки, освіти, культури, соціальної усталеності суспільства, швидко формуються сектори економічної і банківської інформації.

Стосовно наукової і технічної інформації ринкові відносини в класичному розумінні мають значні обмеження, які зумовлені тим, що основним принципом ринку є пряме збільшення прибутків від реалізації продуктів і послуг, за основним законом ринку: «Виробляй тільки те, що сьогодні користується попитом і може бути продане».

Особливість інформаційного ринку наукової і технічної інформації полягає в тому, що:

— значна частина інформації (у формі інформаційних продуктів і послуг) у своїй основі спрямована на забезпечення поінформованості суспільства в цілому, інформаційного забезпечення наукових досліджень і розробок, підтримку процесів підготовки спеціалістів (відтворення кваліфікованої робочої сили) і т. п., а не на одержання прямих доходів і прибутків. У зв'язку з цим виникає перша суперечність між соціальною функцією інформації і її недоступністю внаслідок різних причин, зокрема, установлення високих цін, відсутності каналів зв'язку й ін.;

— інформація може бути затребувана як на теперішньому відтинку часу, так і через досить тривалі періоди, тому має здійснюватися функція зберігання інформації, яку забезпечують бібліотеки, архівні служби і т.п.

Тут виникає друга суперечність, пов'язана з оперативністю інформування суспільства про нові досягнення і з цілісністю інформації як національного інформаційного ресурсу, що забезпечує потенціал країни в майбутньому;

— інформація за своєю суттю інтернаціональна. Для неї не існує державних кордонів, оскільки розвиток телекомунікацій зумовлює їх вільне перетинання. Закріплення інформації у формі продукту на тому або іншому носії не означає, що власне інформація не може бути передана в ході бесіди, дискусії, повідомлення на конференції. Так виникає третя суперечність — між відкритістю інформації як такої і прагненням різноманітних суспільних утворень (на рівні держави, фірми) не дати стати надбанням громадськості частині інформації з тих або інших причин.

Інтернаціональна природа інформації зумовлює те, що ринок інформаційних продуктів і послуг не може орієнтуватися винятково на комерційні принципи і бути замкнутим у рамках офіційних кордонів держави, він характеризується максимальним ступенем відкритості, цьому сприяє і розвиток телекомунікацій. Поглиблення і посилення зв'язків між національними індустріями інформації, зростання їхньої взаємозалежності і взаємодоповнюваності визначають об'єктивність існування світового інформаційного ринку.

У таких умовах посилюється роль держави, що має взяти на себе відповідальність за державний сектор інформаційної структури України, маючи на увазі підтримку процесу розвитку національного інформаційного ринку за оптимального поєднання ринкових і регульованих державою механізмів поширення інформації.

У діяльності служб наукової і технічної інформації колишнього СРСР увага була зосереджена на вирішенні завдань збору, перероблення, пошуку і збереження інформації, а процеси комунікації значною мірою регламентувалися. Інформаційне обслуговування як «вибіркове поширення інформації» (ВПІ) і ретроспективний пошук (РП) забезпечувалися за встановленими державою цінами. У системі циркулювали величезні потоки інформації, генерувався «інформаційний вал» за дефіциту потрібної інформації. Виробники інформації придушили пріоритет споживачів, внаслідок чого споживач одержував не ту інформацію, що йому була потрібна, а ті відомості, що визначалися доступним йому рівнем і можливостями системи.

Узагалі на ринкових принципах не працює інформаційна структура в жодній країні. Це пов'язано з великими витратами на формування інформаційних продуктів і послуг, зокрема у сфері наукової і технічної інформації, оскільки значною мірою орієнтовані на комунікації в неринкових секторах економіки (наука, освіта, культура). Вкладаючи кошти в інформаційну діяльність, держава виходить із того, що результати цих вкладень належать державі, а отже, громадянам країни без будь-якої оплати, тому що створені за їхній рахунок. На жаль, це призводить до того, що безоплатна або пільгова реалізація інформаційних продуктів і послуг, зроблених за рахунок держави, порушує свободу конкуренції для недержавних учасників інформаційного ринку і розв'язання цієї проблеми потребує координування з боку держави.

Проблеми інформаційних технологій відбиваються в усіх конфліктних ситуаціях сучасного вирішення прав суб'єктів на результати інтелектуальної власності і зачіпають питання про роль держави в забезпеченні прав багатьох суб'єктів відносин у даній сфері. Це стосується як безпосередніх створювачів цього продукту, так і прав власників, на кошти яких створюється про-

дукт, прав держави в цій галузі в тому числі, користувачів продуктом.

Усі доктрини і концепції, реальна діяльність держав США, Німеччини, Франції, Японії та інших розвинутих країн у галузі забезпечення розвитку інформаційних технологій (концепції Клінтона — Гора, Бангемана в Європі, Окінавська хартія глобального інформаційного суспільства і т.д.), доктрина інформаційної безпеки Російської Федерації охоплюють великий спектр проблем, що стосуються активного втручання держави в сферу відносин, що розглядається.

Специфіка сучасного періоду полягає в тому, що всі зміни в інформаційній сфері відбуваються в історично стислі строки. На очах одного покоління протягом 30 — 40 років інформаційно-пошукові системи на картах із крайовою перфорацією перетворилися на наймогутніші телекомунікаційні мережі, здатні обробляти величезні масиви інформації й передавати їх по всій земній кулі.

Сьогодні локомотивом розбудови інформаційного середовища розвинутих країн виступають найбільші комп'ютерні корпорації, а головним інтегруючим елементом нової світової інформаційної інфраструктури, її сутністю є Всесвітня мережа, яка дає змогу об'єднувати інформаційні ресурси національних інформаційних систем.

Глобальна інформаційна мережа, що стала найбільш значним технологічним нововведенням ХХ століття і дала змогу ефективніше використовувати світові інформаційні ресурси, зумовила неформальні творчі контакти фахівців, стала одним із найбільш діючих чинників розвитку науки і освіти. Галузь інформаційних технологій і телекомунікацій робить дедалі значний внесок у розвиток економіки розвинутих країн, вони стають рушійною силою не тільки бізнесу, а й соціуму в цілому (рис. 5). Однак припущення про єдиний світ без кордонів і урядів, у якому індивідуальна свобода захищена лише засобами криптографії, навряд чи мають шанс коли-небудь реалізуватися.

Технічні, або техніко-технологічні, універсальні і спеціалізовані засоби обробки інформації становлять інформаційну інфраструктуру (ІФС) держави. Навіть фахівець інформаційної служби при опрацюванні в ручному режимі умовно стає елементом інформаційної системи, не кажучи вже про те, що становлен-

ГД—і—і—1⁰⁰
 ө _га 5 ^ <о х
 о % \ г-- х
 t ^"R и Ш - В,
 ^ ий т- _ и м

Ц~\<в s " § i
 Й j ^ ^ n R R o l S

•aiI Лii* * TI Ъ1«1лTiaI 8 I
 i ? f < f l i g ^ f i k l f f e a i j i l l 3 i
 UPifiiiUffsiiffUIH < i
 II IMUI II IHU1 IUUMUMUUN1 | м н й ° I I

If J | _ | > ; | ^ | _ E > ^ ^ ^ ^ 1 ; _ _ « I ' i
 if > я ' > £ / * • : > > Ц и с Ъ / I S
 § g - < / _ _ _ • > • - y _ _ _ > Ъ = ! * _ _ o £ л
 If < s t ^ / ' > H / - i « I . • - i I

Я _ If III 111 § у
 ^ E—O—Br* ч
 НИи 1»

ня інформаційного суспільства супроводжується новим масовим явищем — людиною, яка подорожує без кордонів, із трубою мобільного телефону. Абонентська щільність і територіальне охоплення безпроводного зв'язку досягли системоутворюючого рівня в побудові інформаційних інфраструктур. Гасло мобільного радіосервісу (MPC) третього (3G) і четвертого (4G) поколінь — «зв'язок будь-який, завжди, скрізь» — підкреслює постійно і швидко зростаючі потужності інформаційної оснащеності і можливості інформаційної взаємодії «безпроводної» особистості. Масовість і динамічний стан (вільне переміщення без кордонів) цих особистостей не вписуються в традиційне уявлення інформаційного забезпечення, у традиційні структури об'єктів інформатизації у вигляді певної кількості стійких робочих місць.

Інформаційна оснащеність і можливості інформаційної взаємодії людини, що подорожує із «трубкою» по радіоінтерфейсу, пропорційні або перевищують можливості традиційних об'єктів інформатизації. Відповідно на них має бути поширена нормативна метрика інформаційного забезпечення, включаючи інформаційну безпеку, захист інформації і видів інформаційних загроз. Подорожуючий портативний ноутбук із глобальним інтерфейсом радіодоступу, що одержує і переробляє значні за обсягом інформаційні ресурси, в сучасному світі стає некерованою інформаційною бомбою і не може бути поза сферою інформаційного моніторингу.

Обробка інформації автоматизованою системою не повинна змінювати змісту вхідної інформації. На цьому положенні, зокрема, базуються всі законодавчі та нормативні документи, які регламентують процеси обробки інформації. У ст. 1 Закону України «Про захист інформації в автоматизованих системах» визначена: «Інформація в АС — сукупність усіх даних і програм, які використовуються в АС незалежно від засобу їх фізичного та логічного представлення. Обробка інформації — вся сукупність операцій (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація), що здійснюються за допомогою технічних і програмних засобів, включаючи обмін по каналах передачі даних». Інформація захищається авторським правом, що ще раз підкреслює її суть — змістовність.

Рівень ресурсів, пов'язаний з інформаційними системами, щонайтісніше пов'язаний з політикою інформатизації, його

характеризують такі основні елементи, як власне постановка завдання щодо створення змістовної інформації, людей, які мають ці завдання виконувати, створюючи програмно-технічне забезпечення, внутрішні правила та положення і, безумовно, технічний захист інформації, який сам по собі є досить складною і самостійною проблемою.

Інформатизацію в Україні було розпочато створенням відомих інформаційних систем. Кожна державна установа, науководослідний інститут, інформаційно-обчислювальний центр, підприємство, незалежно від розмірів та форми власності, з набуттям незалежності почали створювати необхідні для своєї діяльності бази даних. На жаль, через розрізненість та хаотичну актуалізацію вони не дають повної картини про стан національної інформаційної ресурсної бази (табл.1).

Таблиця 1
Відомості про тематичний розподіл баз даних

Тематика	Роки						
	1991	1993	1995	1997	1998	1999	2000
	КІЛЬКІСТЬ						
Бізнес	2101	2644	2769	2887	3014	3039	2829
Споживча інформація	450	837	978	1082	1343	1680	1725
Медицина і біологія	690	742	775	826	1004	1154	1286
Гуманітарні дисципліни	248	330	367	432	526	626	629
ГОЛОТЕМАТИЧНІ	366	230	209	254	354	465	500
НАУКОВО-ТЕХНІЧНА інформація	1210	1529	1568	1635	1749	1889	1937
Суспільні науки	453	473	495	557	619	638	623
Новини	291	369	421	473	476	503	498

Верховна Рада України оперує базами даних про склад та структуру парламенту, зміни, що вносяться до Конституції та інших законів, які містить база даних «Законодавство України».

Кабінетом Міністрів України розроблені та супроводжуються бази даних про склад уряду, законодавче забезпечення соціально-економічної політики, єдиний державний автоматизований паспортний реєстр.

У Головному управлінні державної служби України функціонує база даних «Реєстр контрактів з керівниками державних підприємств, установ і організацій та головами правлінь акціонерних товариств, контрольний пакет акцій яких належить державі».

У Міністерстві закордонних справ України підтримуються бази даних по структурах міністерства з питань зовнішньополітичної діяльності України: новини, заяви, виступи та прес-релізи з усіх аспектів зовнішньої політики України.

У Міністерстві освіти і науки України функціонують бази даних про навчальні заклади України, навчання за кордоном, про новини науки, про вищі та середні спеціальні навчальні заклади, спеціалізовані дитячі установи.

Структури, підпорядковані Міністерству праці та соціальної політики України, також мають багато інформаційного матеріалу. Пенсійний Фонд України користується у своїй роботі автоматизованою системою обробки документації по пенсіях та допомогах (АСОД/КОМТЕХ). До складу цієї системи входить більше 90 автоматизованих робочих місць (АРМ). Інформація, що накопичується в базах даних, дає змогу одержати довідки про кількість пенсіонерів-інвалідів м. Києва; про пенсії льотних екіпажів; особові рахунки; про прибутки пенсіонерів тощо. Управління соціального захисту населення, Фонд інвалідів використовують інформацію, що накопичується в базі даних «Наша сім'я» (облік громадян України, які потребують соціальної допомоги).

Міністерство екології і природних ресурсів України супроводжує базу даних про стан навколишнього середовища та екологічні проблеми України.

Міністерство юстиції України супроводжує бази даних про апарат міністерства, місцеві управління юстиції, судову систему, нотаріат, інститути судової експертизи, «Законодавство», «Нормативні акти України», «Лоцман».

В Українському інституті науково-технічної та економічної інформації функціонує банк даних, який об'єднує понад 4000

українських веб-сайтів, що розбиті за тематичним та алфавітним каталогами. З 1992 року інститут веде базу даних зареєстрованих НДДКР та дисертацій, яка на сьогодні налічує більш як 420 тисяч документів, а з 1998 року проводить реєстрацію електронних інформаційних ресурсів з науково-технологічної та економічної діяльності.

Інститут проблем реєстрації інформації (ІПРІ) НАН України розробив та впровадив метабазу даних «Реєстр інформаційних ресурсів м. Києва» (РІР). База розміщена в Інтернеті на веб-сервері (www.ipri.kiev.ua). Крім того, ІПРІ НАН України містить інформацію про бази даних, які накопичені в органах державної влади та місцевого самоврядування м. Києва.

Обласні та міські адміністрації України розробили та супроводжують бази даних про нормативно-законодавчі загальнонаціональні та регіональні документи, статистичні та економічні показники розвитку регіонів, міграцію населення, служби зайнятості, тендери, культурно-оздоровчі заклади, банки тощо.

В Україні розпочата робота по розробці системи електронних бібліотек. Першою такою системою в Україні стане електронне об'єднання трьох провідних бібліотек України: Національної бібліотеки України ім. В. І. Вернадського, Парламентської бібліотеки та бібліотеки Київського національного університету імені Тараса Шевченка.

Специфіка завдань, що вирішуються за допомогою ІС, різна складність їх побудови, модифікації, супроводження, інтеграції з іншими ІС тощо, розділили інформаційні системи на: відкриті (для загального користування) або закриті (для обмеженого доступу); державні або недержавні; національні або міжнародні; малі, середні, великі. Їх створення вимагає системно оглянути всі етапи проектування та реалізації автоматизованих систем у цілому, програмно-технічних засобів, які забезпечують обробку ЗІР відповідно до визначеної мети; підвищити вимоги до експлуатації систем обробки та передачі інформації згідно із світовими технічними нормами.

Розглядаючи проблеми створення в Україні інформаційного ринку, можна стверджувати, що, оскільки держава не змогла взяти під контроль створення інформаційної інфраструктури в окремих регіонах, галузях, виробництвах, процес в Україні розвивається сьогодні досить стихійно, але його структура не

може істотно відрізнятись від тих моделей, що вже сформувалися в розвинутих країнах в умовах ринкової економіки, оскільки на даному етапі вирішується головне завдання інтеграції вітчизняної інформаційної інфраструктури у світовий інформаційний ринок. Це стимулюватиме конкурентоспроможність наших пропозицій світовим постачальникам інформаційних послуг, підтримку прогресивних форм і методів використання інформаційних ресурсів з урахуванням тенденцій розвитку світового ринку, посилення співробітництва і солідарності в проведенні політики у сфері інформаційних продуктів і послуг.

У розвинутих індустріальних країнах Європи і США створена потужна інформаційна індустрія із своєю технологією, системою підготовки кадрів, нормами та стандартами, методами управління та маркетингу, засобами доставки інформації. У цих країнах продукти інформаційних технологій є товаром, сформувався інформаційний ринок, який дедалі більше втягує в свою орбіту і Україну.

У США створена інформаційна інфраструктура, що забезпечує доступ до загальнонаціональних інформаційних ресурсів з будь-якого куточка країни; на її основі комп'ютеризовані практично всі сфери суспільної діяльності. Інформатизація у США здійснюється згідно з програмою «Стратегічна комп'ютерна ініціатива», основною метою якої є створення нового покоління комп'ютерів — з високим інтелектом.

Усвідомлюючи зростаючу перевагу США на ринку інформаційних технологій, Європейський Союз починає активні дії, спрямовані на подолання відставання в цій сфері. Наприкінці 1999 року ЄС розробив стратегію розвитку «європейського інформаційного співтовариства». Активізує свою діяльність в цьому напрямі Японія, де відповідно до прийнятої програми інформатизації також інтенсивно ведуться роботи зі створення ЕОМ, в яких має бути реалізований штучний інтелект. Водночас нові комп'ютерні телекомунікаційні технології дали змогу перейти до формування проекту «Нові рубежі людства» на базі дослідження принципів, що лежать в основі функціонування живих систем, і їх впровадження для цілей нових технологій, систем, автоматів, систем керування тощо.

Національну політику в галузі інформаційних технологій розробили Китай, Індія та ряд інших країн. Цікавий у зв'язку з

цим приклад Індії, яка протягом останнього десятиліття створила індустрію програмних продуктів, спрямовану на експорт і кооперацію з найбільшими телекомунікаційними компаніями. За наявними оцінками, капіталізація індійських компаній у 2000 році перевищила 25 млрд. доларів, а обсяг експорту програмних продуктів досяг 3 млрд. доларів.

Місце Росії у світовому інформаційному просторі залишається незначним, що не відповідає її претензіям на статус великої держави і наявному культурному і науково-технічному потенціалу. Російська влада це усвідомлює. Зокрема, Президент В. Путін в одному із виступів зазначив, що обговорення теми високих технологій у Росії «пожвавилось, але, на жаль, рівень розвитку нової економіки ще не відповідає її важливості для країни», у країні стався розрив між можливостями держави в розвитку нових технологій і потребами бізнесу в цій сфері.

Федеральна цільова програма «Електронна Росія (2002 — 2010 роки)», яка була прийнята Урядом РФ у січні 2002 року, визнаючи за необхідність опрацювати конкретні шляхи реалізації ідей глобальних інформаційних систем в умовах своєї країни, поставила за мету забезпечення нормативної бази інформаційних і комунікаційних технологій, розвитку інформаційної і телекомунікаційної інфраструктури, сформувати умови для підключення до відкритих інформаційних систем, зокрема до Інтернету, а також забезпечити ефективну взаємодію місцевого самоврядування з громадянами і структурами державного і приватного господарства.

В інформаційному суспільстві змінюються і функції державного управління. Дедалі зростаюча частина часу чиновників і державних бюджетів направлятиметься на створення мегабаз даних національного і наднаціонального масштабу, на управління інформації, що утримується в них, удосконалення каналів і засобів її збору і поширення, тому вимоги економічності, розумної достатності й ефективності інформаційних технологій, які застосовуються, зумовлюють необхідність системного підходу до цієї теми.

РОЗДІЛ 2

ОРГАНІЗАЦІЙНО-ПРАВОВІ МЕХАНІЗМИ ВІДТВОРЕННЯ НАУКОВОГО ПОТЕНЦІАЛУ В НАЦІОНАЛЬНОМУ ЗМІСТОВНОМУ ІНФОРМАЦІЙНОМУ РЕСУРСІ

2.1. ІНФОРМАЦІЙНА СКЛАДОВА НАУКОВО-ТЕХНІЧНОЇ ПОЛІТИКИ ДЕРЖАВИ

Упродовж останніх десятиліть ХХ століття у становищі науки і техніки в суспільстві відбуваються суттєві зміни. Відповідно змінюються і місце та роль науково-дослідної діяльності. Ці зміни насамперед стосуються:

- обсягу асигнувань, що виділяє суспільство на розвиток наукових досліджень;
- практичного використання їх результатів;
- ролі та вагомості досліджень і розробок як чинника економічного розвитку;
- частки продукції високих технологій у загальному обсязі промислового виробництва;
- частки участі приватного сектору в розвитку наукових досліджень;
- зв'язку та взаємодії вищої школи та промисловості;
- використання венчурного капіталу;
- ролі регіонів у розвитку наукових досліджень і розробок;
- розширення міжнародної наукової співпраці.

Наука виконує дві основні функції: культурну, що пов'язана із впливом на людину та її уявлення про навколишній світ, та практичну — передусім технологічну та економічну, оскільки технологія дедалі більшою мірою ґрунтується на досягненнях науки. Значення практичної функції науки невпинно зростало упродовж століть, а з 80 — 90-х років ХХ століття цей процес особливо пришвиджується.

З плином часу було усвідомлено, що цей чинник діє не довільно, а тільки в поєднанні з іншими, зокрема такими, як розвиток зовнішньої торгівлі, що в умовах глобалізації економіки і створення міжнародних зон вільної торгівлі стає чинником економічного розвитку, та, окрім того, з такими, як ефективність досліджень і розробок, виробництва, банківської діяльності.

Значне розширення частки участі приватного сектору в наукових дослідженнях і розробках передусім проявляється в таких сферах, як приватизація науки та її комерціалізація. Ця тенденція однаковою мірою охоплює фінансування наукових досліджень і менеджмент у галузі досліджень та розробок. Це стосується навіть великих військових науково-дослідних програм, що здійснюються, наприклад, у таких країнах, як Франція та Велика Британія.

Що ж до комерціалізації науки, то спостерігається загальносвітова тенденція до постійного зростання частки результатів наукових досліджень, які є предметом купівлі-продажу (навіть у своїй «нематеріальній» формі).

Зв'язки між вищою школою, промисловістю та їх втіленням набувають найрізноманітніших форм. У сфері досліджень вони реалізуються як створення технопарків, організація спільних підприємств, укладання коротко- та довготермінових угод, створення в галузях високих технологій дочірніх (spin-off) фірм працівниками вищої школи для виробництва продукції або надання певних видів послуг; створення спеціалізованих у галузі права і технологій інформаційних центрів, що сприяють трансферу технологій; консультування вченими, які працюють у вищій школі, промислових підприємств.

Використання терміна «венчурний капітал» (капітал ризику) зазвичай окреслює та визначає капітал, який пов'язаний з перспективами великих прибутків, з одного боку, та з невизначеним (тобто таким, де не можуть бути апіорі враховані вагомі фактори ризику) ризиком — з іншого. Підприємства, що займаються комерційною апробацією науково-технічних новацій отримали назву венчурних фірм. До них належить переважна більшість малих та середніх фірм у наукоємних галузях економіки розвинутих країн. Розрізняють дві організаційні форми венчурних фірм: всередині однієї компанії та самостійні венчурні фірми. Останні, як правило, працюють на консолідованих заса-

дах (Наприклад, ще з кінця 80-х років у Німеччині таку діяльність провадять об'єднання *Wagnisfinanzierungs Gesellschaft*, до якого входять 27 банків, та *Techno Venture Management Gesellschaft*, що є спільним підприємством фірм *Siemens*, *Bauer*, *Messerschmidt*, *Deutsche Bank* та трьох фондів венчурного капіталу. У Франції поряд з іншими діє національне агентство *ANVAR* (*Agence nationale pour la valorisation de la recherche*). У межах ЄС діяльність за такою формою підтримувалась *Venture Capital Association*)¹²⁸. Фонди венчурного (ризикового) характерукладаються у виробництво на початковій фазі діяльності невеликих фірм, що спеціалізуються на реалізації нових ідей та новітніх технологій. Венчурний капітал не обмежується наданням новим фірмам фінансових засобів. У таких випадках передбачається також сприяння у надбанні навичок, необхідних для успішної підприємницької діяльності, у розробці планів маркетингу, розвитку фірми та керівництва нею. Кредити або внески великих компаній вкладаються у венчурний бізнес без будь-якого матеріального забезпечення та гарантій з боку «венчура» (фірми, в яку вкладаються кошти). Тому інвестори йдуть на серйозний ризик: у разі неуспіху в науково-технічних розробках вони втрачають значні ресурси. Створення венчурної фірми передбачає наявність чотирьох складових¹²⁷: ідеї нововведення (нового продукту, технології, послуги); суспільної потреби в даній інновації; підприємця, що готовий на підставі такої новації створити венчурну фірму; венчурного (ризикового) капіталу для фінансування цієї фірми. І в Європі, й у США потенціал нових технологій у таких галузях, як електроніка, комп'ютеризація, комунікація, генна інженерія, фармацевтична промисловість здебільшого був створений саме завдяки інвестиціям такого характеру, а в наш час така практика набула найбільшого поширення. Ці інвестиції здійснюються спеціальними відділеннями державних або комерційних банків, а також через створювані з цією метою спеціальні фонди. У багатьох країнах таким інвестиціям надається підтримка, для чого використовуються громадські фонди; банкам надаються державні гарантії по кредитах, фірмам — у початковий період їх діяльності — пільги при оподаткуванні.

Розвиток регіональних (міжнаціональних) ініціатив у галузі досліджень та розробок, як правило, підтримується регіональ-

ними владами, які надають підтримку розвитку зв'язків між промисловістю та вищими навчальними закладами своїх регіонів, що сприяє створенню регіональних наукових центрів високого рівня. За приклад може слугувати міжуніверситетський центр мікроелектроніки у Левені (Бельгія), що поєднує наукові колективи Левенського, Гентського та Брюссельського університетів і фінансується фламандськими владними органами. У країнах Скандинавії регіональний підхід здійснюється з кінця 80-х років і є нині головним фактором, що впливає на формування національної наукової політики. У Франції таку роль відіграють регіональні центри інновацій та трансферу технологій. Набувають розвитку регіональні ініціативи і в інших країнах, у тому числі спільні. Ці ініціативи мають досить різноманітний характер. Іноді вони розвиваються у рамках більш широкої політики децентралізації в даній країні, в інших випадках їх метою є поживавлення економіки конкретного регіону. Прикладом останнього є наміри Уряду Російської Федерації здійснювати саме таку політику, що оформлено федеральним Законом «Про статус наукограда Російської Федерації»¹²⁸.

Однією з характерних особливостей науки завжди був інтернаціоналізм. Новизна сучасної ситуації полягає в тому, що індустріально розвинуті країни систематично стимулюють розвиток міжнародного співробітництва в галузі науки і техніки, що переважно виступають як ініціатори, призначають для цього спеціальні фонди. Кошти з цих фондів використовуються для фінансування обміну науковцями, розвитку двостороннього співробітництва, участі у міжнародних системах наукової кооперації.

Про розширення міжнародних наукових зв'язків свідчать, зокрема, результати бібліометричних досліджень, які відображають зростання кількості спільних публікацій авторів, які працюють у різних країнах. Таке явище є похідним від дії багатьох чинників, у тому числі таких, як глобалізація економіки, зростання кількості міжнародних науково-дослідницьких програм, розвиток технологій обміну інформацією тощо. У багатьох випадках при цьому ініціаторами разом з урядом виступають окремі науково-дослідні центри, університети та інші вищі навчальні заклади, а також окремі вчені. У зв'язку з цим можна відзначити, що останніми роками спостерігається:

- зростання кількості досліджень і розробок, які проводяться зарубіжними фірмами в країнах, що інвестуються;
- розширення зв'язків між національними науковими центрами та зарубіжними фірмами;
- розвиток міжнародного співробітництва у проведенні досліджень і розробок на наднаціональному рівні;
- зростання кількості угод про спільні дослідження та розробки між двома або кількома фірмами.

Стосовно держави та її ролі у розвитку науки в контексті описаних змін мають бути отримані відповіді поряд з іншими і на питання про те, у чому має полягати роль держави в розвитку технологій: у фінансуванні розробок, які можуть дати найбільший економічний ефект, чи у створенні фіскальних та правових умов, що стимулюють інновації, при одночасному покладанні відповідальності за вибір технологій на фірми, які найкраще орієнтуються в тому, яка з цих технологій може мати комерційний успіх?

Стає цілком зрозумілим, що відповідь на таке запитання залежить від визначення чинників, які впливають на його прийняття, а саме — від централізованості планування та управлінських рішень, що встановлюють економічні фактори здійснення прийнятої стратегії.

У різних країнах органами, до компетенції яких належать питання науково-технологічної та економічної політики, використовуються різноманітні та численні критерії встановлення стратегій розвитку, найвагомішими серед яких вважаються такі¹²⁹:

- відповідність державним завданням (зміцнення військового та економічного потенціалу держави);
- значущість з погляду розв'язання найбільш важливих соціальних проблем, таких, наприклад, як забруднення навколишнього середовища, зростання злочинності, наркоманія;
- потенціал експансії нових наукових дисциплін (таких, наприклад, як молекулярна біологія та генна інженерія);
- наявність у країні досить розвинутих наукових шкіл.

На прийняття конкретних рішень впливають також особливості національно-культурної спадщини даної країни, актуальні політичні інтереси, наукові традиції, географічне розташування, рівень розвитку виробництва.

У більшості країн з перехідною економікою, в тому числі в Україні, склалася ситуація, коли відмова від планово-централізованої економіки і ринкова лібералізація економічного життя здійснюються без одночасної узгодженої переорієнтації виробництва на нові джерела економічного зростання — наукові знання, нові технології, ефективне використання світового інформаційного простору, що об'єктивно зумовлює формування економіки перерозподільного типу. Така економіка неспроможна конкурувати на сучасному світовому економічному ринку, забезпечувати нарощування національного багатства, оскільки не має для цього сучасного відтворювального потенціалу.

Загальна економічна криза, якої зазнала Україна упродовж останнього десятиліття, супроводжувалася зменшенням виробленого валового продукту і поглибленням дефіциту державного бюджету, що в свою чергу зумовило і скорочення бюджетної фінансової підтримки науки. Рівень бюджетних видатків на науку зменшився.

Політично проголошені цільові пріоритети все ще не повною мірою переросли в реальну політику, що впроваджується державою в сферах промислового виробництва, фундаментальної та прикладної науки, освіти, інформатизації тощо. Це доводить і кількість вітчизняних науковців, що суттєво поступається рівню багатьох країн і надалі зменшується (Так, за міжнародною базою даних SCI, яка містить інформацію щодо публікацій у 5693 журналах з природничих наук (більше третини — журнали США і лише 11 українських журналів), частка публікацій українських вчених у 1992 році становила 0,78%, надалі зменшувалась і в 1998 році становила 0,46%)¹³⁰.

У сучасній економіці відносини інтелектуальної власності (ІВ) посідають своє певне місце, активно впливаючи на форми розвитку сучасного технологічного способу виробництва. Саме оптимізація відносин власності, їх досконалість визначає рівень соціально-економічного потенціалу на макро- і мікрорівні. У промислово розвинутих країнах на сьогодні інтелектуальне виробництво стає одним з основних важелів економічного зростання і становить до 60% у його загальному обсязі. Об'єктивно все це зумовлює необхідність принципово нового типу стабільного відтворення, заснованого на функціонуванні науки, осві-

ти, інформаційних сфер — усього того, що забезпечує активний розвиток інноваційних процесів у суспільстві.

Характеризуючи рівень досліджень відносин інтелектуальної власності, слід наголосити, що дослідження цієї проблеми не мають комплексного і систематизованого характеру. Економіка інтелектуального виробництва вивчалася ізольовано від економічної системи в цілому, не розглядалися такі системоутворюючі категорії, як власність, тобто відносини інтелектуальної власності та механізм їх реалізації. При аналізі інтелектуальної власності переважає формально-юридичний підхід¹³¹. При оцінці результатів інтелектуальної діяльності трудова теорія вартості не завжди виявляється раціональною тому, що не враховує впливу результатів інтелектуальної творчості на величину вартості кінцевого продукту.

Спостерігаються також структурні зміни у пропозиції інтелектуальних продуктів на ринку об'єктів ІВ України: зростання частки інтелектуальних продуктів, пов'язаних зі створенням товарів широкого вжитку і технічно складних послуг; зменшення частки інтелектуальних продуктів, спрямованих у промислові (базові) галузі, і як наслідок — зменшення базових інновацій.

Національний науково-технічний потенціал, який становить підґрунтя пропозиції на ринку інтелектуальних продуктів України, має досить невиразну перспективу через незадовільні умови виявлення попиту та захист як інтелектуальної праці, так і науково-технічної продукції.

Відомо, що включення відносин інтелектуальної власності до сфери матеріального виробництва відбувається у ХІХ столітті: здійснюється юридичне оформлення інституту ІВ шляхом становлення авторського та патентного права, в основу якого була покладена функція здійснення права власності на засоби виробництва, тому що тільки її наявність забезпечувала власнику інтелектуального продукту розпорядження своїм товаром на ринку.

Науково-технічна революція (термін з'явився у 50-х роках ХХ століття) ознаменувалася глибинними процесами інтеграції науки у виробництво, гуманізацією суспільства, зростанням його інтелектуального потенціалу. Необхідність реалізації науково-технічних досягнень зумовила розробку окремих фундаменталь-

них положень теорії ІВ (акумуляція наукового знання, якісний склад робочої сили та роль зростання її кваліфікації, теорія людського капіталу, індустрія, знань тощо). Паралельно з кінця 60-х років ХХ століття відбувається повсюдний процес створення державної інфраструктури підтримки процесу впровадження науково-технічних досягнень у виробництво — організація системи науково-технічної інформації, яка не замінює, а лише підсилює процес поширення знань та виробничого досвіду з погляду можливостей володіння, користування, розпорядження об'єктами новаций, втілених у науково-технічному доробку індивідуалізуючих її суб'єктів.

Специфічна особливість науково-технічних новацій як інтелектуальних продуктів на сучасному етапі становлення нашої держави полягає в тому, що вони відповідають потребам користувачів за своїм змістом (змістовною інформацією), а пропонуються на ринку в об'єктивованій формі. Тому визначати ознаки та межі товарності інтелектуального інформаційного продукту (ПП) (чи продукту інтелектуального виробництва) дуже складно, оскільки при операціях купівлі—продажу (чи надання обміну) не спостерігаються риси, притаманні звичайній товарній продукції. Не відбувається також повного відчуження ПП, а лише його матеріального носія. Сам же продукт, особливо у вигляді даних чи відомостей щодо його науково-технічної суті, можна використовувати велику кількість разів. Механізм отримання прибутку чи просто корисності від надання його у господарський обіг або при комерціалізації результатів науково-технічної діяльності стає можливим за умови створення певних правових гарантій та проведення відповідної державної політики. Державна політика щодо визначення умов створення і поширення інтелектуальних продуктів як результатів науково-технічної діяльності стосується економічних, соціальних та інформаційних аспектів їх використання.

Розвитком відносин ІВ виступає процес соціалізації, оскільки ПП перебувають у безпосередній залежності від їх корисності для суспільства, і вони в такий спосіб включаються у ринок. Ринкова система стає засобом відбору, оцінки та критерієм корисності інтелектуальних продуктів.

Юридичні обмеження щодо загального використання ПП з метою досягнення максимальної економічної ефективності по-

в'язані з такими чинниками, як визнання та підтвердження права самостійного використання їх власником, передача в тимчасове використання за певну плату, продаж у повне володіння іншому суб'єкту.

Суб'єктами інтелектуального виробництва можуть виступати: сам виробник ІШ, приватний капітал та держава. Звідси впливають різноманітні організаційні форми надання в суспільний (економічний) обіг самого інтелектуального продукту, оскільки ці форми відображають реально існуючі суспільні групи, що беруть участь у процесі створення та поширення інтелектуального продукту: індивідуальна (особиста), приватна, державна, кооперативна, акціонерна, змішана форми.

Кожен із суб'єктів претендує на певну частину прибутків від реалізації інтелектуального продукту або ІШ, які також можуть набувати різної форми — заробітної плати; прибутку від комерційної реалізації об'єкта інтелектуальної власності його власником (чи експлуатації цього об'єкта); відсотка, який виплачується власнику інтелектуального продукту за користування цим продуктом іншою особою.

Таким чином, науково-технічні досягнення, що набувають об'єктивної форми інтелектуальної власності у вигляді інтелектуальних чи, більш повно, інформаційно-інтелектуальних продуктів, стають економічною формою розвитку продуктивної сили, яка стимулює переважно індивідуальну інтелектуальну працю.

За світовими стандартами інтелектуальна власність тяжіє більше до приватної власності. Її специфіка полягає в тому, що вона виступає як приватна власність, але водночас не виключає приватно-колективного, державного і міжнародного привласнення залежно від суб'єкта власності¹³².

Для всебічного усвідомлення права власності на інформаційні ресурси, в тому числі права інтелектуальної власності, доцільно звернутися до римського цивільного права, яке було переважно оформлене ще наприкінці II ст. до Р.Х. Як свідчить історія цивілізаційного розвитку, теорія римського інституту права приватної власності не зазнала суттєвих змін донині. Як ґрунтовно доведено¹³³, римське цивільне право є основним джерелом, із якого бере початок світова правова культура. Обсяги і межі права приватної власності римляни визначали за допомогою

правомочності власника, а саме: право володіння (jus possidendi); право користування (jus utendi); право розпорядження (jus abutendi); право отримувати доходи (jus fruendi); право захисту (jus vindicandi). З часом досвід засвідчив, що деякі правомочності певною мірою повторюють одне одного, римляни звужують їх коло. Відпадає така правомочність, як право захисту, оскільки будь-яке право підлягає захисту, а також право користування поглинуло право отримання доходів. Залишилися лише три правомочності: право володіння, право користування, право розпорядження. Вони охоплюють усі можливі форми впливу власника на майно і водночас відмежовують зазіхання інших осіб на це майно. Право власності називають найбільш повним за обсягом, оскільки всі інші права на річ поступаються йому в цьому¹³⁴.

Чинне законодавство України кожному суб'єкту гарантує право володіння, користування та розпорядження його власністю. Однак у сфері права на інформаційні ресурси та права на об'єкти інтелектуальної власності, особливо з питань щодо отримання доходів та захисту цих прав, державні гарантії мають декларативний характер внаслідок відсутності ефективно діючих правових механізмів їх реалізації.

Ефективний захист прав ІВ має сприяти залученню в економіку України іноземних інвестицій та стимулюванню створення національної ІВ. Розвиток законодавства із захисту ІВ є однією з вимог ГАТТ/СОТ та Угоди про партнерство і співробітництво з ЄС. З огляду на посилення політики міжнародної інтеграції протягом 2001 року Україна ратифікувала низку міжнародних угод та доповнила внутрішнє законодавство з питань захисту ІВ. Однак найбільшою проблемою є відсутність механізмів втілення цього законодавства.

Законодавчі та нормативні акти щодо регулювання сфери ІВ та використання ІШ як нематеріальних об'єктів науково-технічної праці можна розподілити на дві групи: а) документи, що регулюють відносини власності; б) документи, які регулюють функціонування ринку ІШ (не самих продуктів як товару). Перша група документів має на меті створити умови для появи ефективного власника, друга — умови для отримання прибутку від інформаційної діяльності. Спільною позитивною рисою документів є те, що вони змінюють курс на ринковий розвиток,

у тому числі суто інформаційної галузі. Спільними недоліками цих актів є їх декларативність, неузгодженість та брак гарантій упровадження. Ухвалені на цей час нормативні акти проголошують ринкову за суттю мету, але не пропонують ринкових заходів щодо її досягнення. Зокрема, в них визначений курс на розвиток підприємств інфраструктури та забезпечення прозорості торговельних операцій. Проте *замість* формування *стимулів* на перший план висунуто питання *контролю*, а надто коли йдеться про забезпечення прозорості торговельних операцій.

Розглянемо сучасні напрями державної стратегії вдосконалення організаційно-правового механізму у сфері створення та використання інтелектуальної продукції як результату науково-технічної діяльності в Україні, інтелектуальної власності в аспекті їх інформаційного відтворення.

Як зазначалося¹³⁵, проект Концепції державної інформаційної політики України передбачає формування державної інформаційної політики лише стосовно засобів масової інформації та видавничої сфери і містить фрагментарні елементи державної інформаційної політики щодо прав на інформацію і свободи інформаційної діяльності. Основні цілі, проблеми, об'єкти і суб'єкти та основні напрями державної інформаційної політики, політика інформатизації та застосування інформаційних технологій розглядаються через призму розвитку сфери масової інформації (друковані ЗМІ, телебачення і радіомовлення, книговидавництва). Лише у п. 4.3, підпункті щодо питань впровадження та використання нових інформаційних технологій визначена необхідність складання єдиної системи розвитку державної інформаційної політики в цій сфері, необхідність аналізу проблем та визначення завдань стосовно формування та функціонування відмінних від ЗМІ гілок національної інфраструктури.

Підходи, на підставі яких розроблено проект концепції, були притаманні державній інформаційній політиці колишнього СРСР, основою якої були агітація і пропаганда, діяльність засобів масової інформації. Інформаційні ресурси щодо результатів наукових досліджень і розробок, матеріального виробництва та інших сфер використовувалися лише в агітаційно-пропагандистських цілях: обґрунтування переваг соціалізму та викривання недоліків і критики капіталізму. Інформаційні ресурси деяких

напрямів досліджень і розробок засекречувалися до 95% від їх загальних обсягів, використання цих ресурсів регламентувалися закритими підзаконними актами. Тобто зазначена сфера була закрита для загального доступу.

Наслідком таких підходів є надто вузьке тлумачення • елементів національного інформаційного простору в державній інформаційній політиці щодо його формування, розвитку та інтегрування у світовий інформаційний простір (п. 3.1) та забезпечення інформаційної безпеки (п. 3.2), а також те, що деякі функції управління інформаційною сферою не врегульовані і не використовуються.

У Концепції державної інформаційної політики України було б доцільним чітко визначити: загальнодержавні (а не тільки стосовно ЗМІ) цілі, принципи, завдання, об'єкти державної інформаційної політики основні напрями діяльності державних органів та інших суб'єктів, що діють у інформаційній сфері щодо забезпечення реалізації політики; організаційні, правові, економічні та інші важелі та механізми її реалізації; визначати напрями впливу на політичний, соціально-економічний, культурний розвиток, забезпечення національної безпеки України та формування інформаційного суспільства. Необхідно було б також чітко визначити об'єкти національного інформаційного простору та принципові питання, пов'язані із забезпеченням його функціонування, розвитку та поступової інтеграції в світовий інформаційний простір.

Принциповими питаннями щодо системи національних інформаційних ресурсів є визначення державної політики, спрямованої на: створення загальнодержавної системи управління СНІР з урахуванням існуючих міжвідомчих, відомчих та регіональних і місцевих систем; впровадження організаційних заходів щодо формування, поширення і забезпечення ефективного використання і захисту інформаційних ресурсів; запровадження фінансово-економічних методів регулювання інформаційної діяльності, облік державних інформаційних ресурсів як майна та немайнових активів, надання інформаційних послуг на безприточковій та комерційній основі. Є також достатньо підстав для включення до класифікатора економічної діяльності нової галузі економіки під назвою «Виробництво інформаційних, ко-

мунікаційних технологій і послуг» з визначенням заходів щодо управління і координації цієї діяльності на рівні державних органів.

Важливими аспектами державної інформаційної політики є визначення напрямів державної діяльності щодо:

- використання науково-технічного і виробничого потенціалу для розвитку всіх елементів національного інформаційного простору;

- формування і регулювання інформаційного ринку (ринку інформації, інформаційних технологій, засобів обробки інформації та інформаційних послуг);

- міжнародне інформаційне співробітництво та інтегрування інформаційно-телекомунікаційної інфраструктури у світові інформаційні системи;

- створення ефективно діючої системи інформаційної безпеки в широкому розумінні цього поняття.

Окремим розділом концепції має бути визначення системи формування і забезпечення реалізації державної інформаційної політики України, в якому необхідно передбачити:

- організаційну структуру державних органів, суб'єктів інформаційної діяльності, що здійснюють законодавчо узгоджену реалізацію державної інформаційної політики;

- функції організаційних структур, здійснювані у процесі реалізації державної інформаційної політики з управління інформаційною сферою;

- повноваження основних суб'єктів господарювання щодо формування механізмів і забезпечення реалізації державної інформаційної політики.

Організаційних заходів, що передбачені у п. 5.4. концепції, та тих, що пов'язані з підвищенням статусу і ресурсних можливостей державного органу влади, а також формування у структурі апарату Ради національної безпеки і оборони України Управління з проблем інформаційної безпеки з мережею представників у регіонах, явно недостатньо для розв'язання сучасних проблем формування і забезпечення реалізації державної інформаційної політики.

Стратегія інформаційного розвитку має враховувати вимоги державної регуляторної політики¹³⁶, яка пропонує нові методичні та практичні підходи до оптимізації, послідовності, передбачу-

ваності та стабільності відносин держави із суб'єктами господарювання. Державне регулювання — це:

- правила і процедури входження в ринок і виходу із нього суб'єктів господарювання, їх створення і ліквідації;

- дозвільна система на проведення певного виду господарської діяльності;

- правила та процедури, що регламентують певні види діяльності, які не підпадають під дозвільну систему;

- контроль за безпекою та якістю продукції;

- контроль за обов'язковими платежами до бюджетів та до державних цільових фондів;

- правила щодо обсягу та процедур подачі обов'язкової звітності;

- регулювання цін;

- антимонопольне регулювання;

- контроль та обмеження щодо грошових та товарних потоків (що стосуються також інвестиційної та зовнішньоекономічної діяльності);

- регулювання зайнятості та використання трудових ресурсів.

Таким чином, регуляторна політика держави охоплює зміст регуляторних актів та сферу адміністративних процедур, зокрема процедури погодження рішень органів влади, консультації з неурядовими організаціями, спостереження за виконанням ухвалених рішень, встановлення адміністративної відповідальності за порушення¹³⁷, в тому числі у сфері державної інформаційної політики.

Для забезпечення економічного зростання методика визначення сектору для проведення регуляторної політики може базуватися на тому, що: саме регуляторний клімат є найважливішим чинником, що стримує зростання в секторі. Іншими словами, потрібно обирати ті сектори, де існують платоспроможний попит та досить розвинута інфраструктура, що якнайкраще відповідає сфері НТІ. Слід підкреслити, що на цю сферу впливають принаймні два чинники: стан законодавчого вирішення питання щодо науково-технічного та останнім часом інноваційного розвитку, а також щодо самої галузі НТІ.

Розвиток інноваційного напрямку у процесі економічної трансформації суспільства проголошено основним принципом держав-

ної політики на сучасному етапі. Але спостерігається непослідовність реалізації цього принципу на практиці:

- кількість вчених-винахідників у науково-технічній сфері становить (на 2000 рік) 13,1% від рівня початку 1990-х років;

- кількість винаходів у розрахунку на 100 тис. населення становила у 1990 році — 35,2, на 1997 рік — упала у 10 разів;

- у 1999 році інновації здійснювали 1,8 тис. промислових підприємств, тоді як у 1998 році — 1,7 тис. Більш сприятливими до нововведень були великі підприємства з чисельністю понад 5 тис. працівників;

- загальний обсяг фінансування технологічних інновацій у 1999 році становив 1,2 млрд. грн. Основне джерело — власні кошти підприємств — 813,8 млн. грн., або майже 70% загального обсягу фінансування. За рахунок держбюджету фінансувалося 10,1% робіт;

- за рахунок залучення інвестицій у 1999 році мали змогу виконувати інноваційні роботи лише 1,6% підприємств (95,5 млн. грн., або 8,2% загального обсягу фінансування);

- кредитами банків користувалися лише 1,3% підприємств, що здійснювали інновації¹³⁸.

На вибір методів державного стимулювання інноваційної діяльності впливають бюджетні ресурси держави; становище провідних національних виробничих об'єднань та підприємств на внутрішньому і світовому ринках, їх здатність виділити достатні кошти для проведення НДДКР; значущість пріоритетних напрямів, визначених органами державного управління; зростання ролі іноземного капіталу як джерела інноваційної діяльності; створення нових організаційних форм виконання спільних досліджень у рамках асоціацій, спільних проектів (виконавці, у тому числі кооперативні та приватні підприємства).

Формування сприятливого економічного середовища на ринку збуту продукції технологій шляхом розміщення економічно вигідних держзамовлень і стимулювання потенційного користувача до її закупки можна назвати найвагомимим із заходів непрямого економічного стимулювання інноваційної діяльності з боку держави. Економічні санкції тоді відіграватимуть стимулюючу та відновлюючу роль: вони передбачаються не тільки для виконавців проекту (програми), а й для органу управління програмою, на випадок несвоєчасного матеріально-технічного,

інформаційного та іншого забезпечення. Фінансові кошти від економічних санкцій можуть перераховуватись у централізований фонд державних науково-технічних програм і використовуватись для покриття витрат, що виникають у процесі реалізації програми. Для державного стимулювання інноваційної діяльності необхідно прийняти ряд законодавчих актів, про які вже давно йдеться, зокрема «Про патентний суд», «Про захист високих технологій», «Про комерційну таємницю».

Вирішення цих питань чи не найбільшою мірою залежить від позицій органів державної влади щодо інформаційної політики, яка реалізується через наявність та адекватність функціонування відповідних організаційно-адміністративних структур, діяльність яких охоплює сферу формування, охорони, зберігання і використання інформаційної продукції за результатами науково-технічної діяльності в Україні, які становлять справжній інтелектуальний здобуток держави.

Сучасними державними структурами, що фахово займаються питаннями власності на науково-технічні здобутки у їх матеріальному та інформаційному аспектах, в Україні є: система охорони інтелектуальної власності; державні центри науково-технічної та економічної інформації, а також організації НТІ; система трансферу технологій, що зараз перебуває в Україні у процесі свого становлення.

2.1.1. Система охорони інтелектуальної власності

Законодавче забезпечення науково-технічної та інноваційної політики фактично почало формуватися в Україні з грудня 1991 року, коли був прийнятий Закон України «Про основи державної політики у сфері науки і науково-технічної діяльності»¹³⁹.

У ньому зокрема окреслювалась процедура затвердження державних науково-технологічних пріоритетів, започатковувалась система державних науково-технічних програм, спрямованих на реалізацію пріоритетних напрямів розвитку науки і техніки, декретувався конкурсний відбір проектів, що входять до складу таких програм. Відповідно до цього закону були створені Державний інноваційний фонд, Державний фонд фундаментальних досліджень, розроблено ряд нормативно-правових актів¹⁴⁰. Брак коштів, ігнорування економічними відомствами

визначених законом, постановами Верховної Ради і указами Президента України пріоритетів призвело на практиці до відсутності забезпечення державної підтримки науки та стимулювання науково-технічної діяльності.

Проект нової редакції закону 1996 року передбачав законодавче забезпечення повернення престижності професії науковця, утвердження його особливого статусу в суспільстві. Законом закріплювалось також запровадження таких інституцій, як Національний науковий центр, науковий об'єкт, що становить національне надбання, хоча їх статус і можливості підтримки не були достатньо опрацьовані. Додатково, у процесі узгодження і редагування, «випали» норми про обов'язковий щорічний звіт уряду про стан науки і технологій, ґрунтуючись на якому Верховна Рада мала б формувати науково-технологічну політику, про відповідальність Кабінету Міністрів за створення сучасної інфраструктури науково-технічної діяльності, про те, що основою для визначення пріоритетів має бути комплексний прогноз соціально-економічного та науково-технічного розвитку України, а також, що під час визначення пріоритетів Верховна Рада має одночасно розглядати питання про їх ресурсне забезпечення, хоча все це було передбачене законом 1991 року¹⁴¹.

Деяким проривом у напрямі законодавчого забезпечення інноваційної діяльності щодо науково-технічної сфери держави можна вважати прийняття у липні 1999 року Закону України «Про спеціальний режим інвестиційної та інноваційної діяльності технологічних парків «Напівпровідникові технології і матеріали, оптоелектроніка та сенсорна техніка», «Інститут електрозварювання імені Є.О. Патона», «Інститут монокристалів»¹⁴². Цим законом жодних пільг безпосередньо для інститутів чи для створення на їх базі комплексів не передбачалось. Спеціальний режим поширюється тільки на інноваційні проекти технопарків, які виконуються в рамках затвердження їм пріоритетних напрямів та належним чином зареєстровані. Це означає, що кожен з таких проектів розглядається Міжвідомчою радою з координації діяльності щодо організації та функціонування технопарків та інноваційних структур інших типів. Серед робіт згаданих інститутів технопарки тощо займають дуже невелику частку.

Проект Закону України «Про інноваційну діяльність» передбачає, що при затвердженні програм діяльності Кабінету Міністрів, загальнодержавних програм економічного, науково-технічного, соціального розвитку чи охорони довкілля Верховна Рада України затверджуватиме в їх складі як загальнодержавну програму пріоритетні напрями інноваційної діяльності, визначатиме обсяг асигнувань для фінансової підтримки такої діяльності в межах держбюджету України, здійснюватиме парламентський контроль за діяльністю Кабінету Міністрів у цій сфері, у тому числі щодо виконання інноваційних проектів, яким надавалася підтримка із державного бюджету¹⁴³.

Для здійснення науково-технічної політики, безумовно, дуже важливим є законодавство про охорону інтелектуальної власності. Закон України «Про охорону прав на винаходи і корисні моделі», прийнятий у 1993 році¹⁴⁴, не вирішував питання повноцінного правового захисту інтелектуального продукту, створеного українськими вченими і винахідниками. Причина полягала в тому, що Україна не мала тоді ні масштабних баз даних, ні розвинутих (або просто окремих) структур, які організаційно забезпечували б патентування винаходів. Держпатент України тоді мав можливість видавати лише передбачені Постановою Верховної Ради України «Про введення в дію Закону України «Про охорону прав на винаходи і корисні моделі» від 23 грудня 1993 року тимчасові патенти на п'ять років без проведення експертизи по суті. Практично ніяких юридичних наслідків для власників таких патентів з володіння ними не впливало. До 1997 року не була створена ні патентно-інформаційна база, ні довідково-пошуковий апарат, необхідні для застосування цього закону, ні загальнодоступна патентна бібліотека. Оформлення ж 20-річних патентів України, що все ж розпочалося, продовжувало залишатися неприпустимо тривалим — до п'яти років. У законі також недостатньо були врегульовані питання захисту прав авторів, які зробили свій винахід, працюючи за наймом, їх взаємовідносини з роботодавцями при комерціалізації винаходів¹⁴⁵.

У 2000 році прийнято нову редакцію Закону України «Про охорону прав на винаходи і корисні моделі»¹⁴⁶, де введено поняття деклараційного патенту, який видається за результатом формальної експертизи на локальну новизну заявки на винахід

на відміну від власне патенту, що може бути виданий лише після глибокої кваліфікаційної експертизи. По суті, це майже той самий «короткий» п'ятирічний патент, який ще можна сприйняти для підтвердження пріоритету, але він не має ніякої вагомості при захисті майнових прав його власника.

Таким чином, не реалізованими залишаються передбачені Конституцією України державні гарантії захисту матеріальних інтересів авторів, що не знайшли свого втілення навіть на рівні підзаконних актів, що робить автора майже стовідсотково залежним від роботодавця.

Відкритий у жовтні 1999 року при Науково-дослідному центрі патентної експертизи Фонд громадського користування надає патентну інформацію цілому ряду країн, проте патентна інформація на електронних носіях надається за кошти, відсутнє реферативне видання «Винаходи країн світу», не вирішується питання забезпечення патентною інформацією в регіонах України.

Своїм указом від 27 квітня 2001 року¹⁴⁷ Президент України зобов'язав Кабінет Міністрів розробити та затвердити програму державного сприяння охороні інтелектуальної власності, спрямовану на формування цивілізованого ринку об'єктів ІВ та забезпечення ефективного захисту прав на такі об'єкти.

Програма розвитку державної системи охорони інтелектуальної власності в Україні на 2001 — 2004 роки серед інших положень містить, зокрема, такі (вибірково — щодо предмета нашого дослідження)¹⁴⁸:

«Розділ 2. Напрямки розвитку державної системи охорони ІВ:

- забезпечення формування та ефективного функціонування інфраструктури, необхідної для реалізації державної політики в сфері ІВ;
- комерціалізація результатів інтелектуальної діяльності, створення цивілізованого ринку ІВ;
- інформаційне забезпечення діяльності у сфері ІВ;
- стимулювання та державна підтримка створення та використання об'єктів інтелектуальної власності».

«Розділ 2.1. Удосконалення нормативно-правової бази:

- підрозділ «Подальший розвиток законодавства України у сфері ІВ базується на таких принципах»:

- оптимальне розмежування та взаємодія публічно-правових і приватно-правових засад для регулювання правовідносин у сфері ІВ;

- забезпечення цілісності та структурної упорядкованості національного законодавства України із законодавством у сфері ІВ;

- забезпечення подальшого розвитку ринкових відносин з урахуванням стану вітчизняної економіки та збереження балансу між її потребами і можливостями;

підрозділ «Реалізація напрямків розвитку нормативно-правової бази» передбачає:

- введення відповідних норм щодо охорони прав на об'єкти ІВ до загального законодавства, а саме до цивільного, кримінального, митного, податкового, антимонопольного, трудового законодавства».

«Розділ 2.2. Забезпечення формування та ефективного функціонування інфраструктури, необхідної для реалізації державної політики в сфері інтелектуальної власності.

(Оскільки цей розділ є головним щодо засад функціонування системи, наведемо його текст повністю):

Участь у формуванні та забезпеченні реалізації політики в сфері ІВ є одним з основних завдань Міністерства освіти і науки України. На виконання цього завдання у складі Міністерства утворено Державний департамент інтелектуальної власності, який є урядовим органом державного управління.

Для здійснення покладених на нього завдань Держдепартамент у встановленому порядку *взаємодіє* з центральними та місцевими органами виконавчої влади, Національною академією наук, іншими академіями наук, творчими спілками, Радою міністрів Автономної Республіки Крим, органами місцевого самоврядування, а також з відповідними органами інших держав. Держдепартамент має здійснювати *керівництво формуванням та розвитком функціональної інфраструктури* державної системи охорони інтелектуальної власності, до якої разом із Українським інститутом промислової власності та Українським агентством з авторських та суміжних прав, які сьогодні включені до сфери управління Держдепартаменту, *мають увійти*:

Апеляційна палата для вирішення спірних питань, пов'язаних з наданням правової охорони об'єктам ІВ;

Державна патентна бібліотека;

Інститут права інтелектуальної власності як базовий навчальний заклад;

Структурні підрозділи з питань інтелектуальної власності, які мають бути утворені у складі деяких регіональних центрів науково-технічної та економічної інформації (ЦНТЕІ), підпорядкованих Міністерству освіти і науки;

пункти державних інспекторів з авторського права та суміжних прав у обласних центрах та великих містах, які увійдуть до складу Українського агентства з авторських та суміжних прав і будуть діяти на комерційній основі.

Для ефективного функціонування такої інфраструктури необхідно встановити *тісне співробітництво із:*

структурними підрозділами з питань захисту прав ІВ, які доцільно утворити у складі МВС, СБУ, Держмитслужби, Державної податкової адміністрації, Мінекополітики та деяких інших органів державної влади;

патентно-ліцензійними підрозділами, які доцільно утворити у складі деяких міністерств та відомств;

Всеукраїнською асоціацією патентних повірених, іншими громадськими організаціями, діяльність яких пов'язана із охороною прав на об'єкти інтелектуальної власності».

Якщо стосовно викладених напрямів розвитку та вдосконалення інфраструктури системи охорони прав на об'єкти інтелектуальної власності практично не виникає питань, то до «комерціалізації результатів інтелектуальної діяльності» (розділ 2.3 програми) під егідою або навіть у межах такої системи є деякі зауваження.

Справді, результати інтелектуальної діяльності мають нематеріальний характер. Це науково-технічні і художньо-конструктивні рішення. Для того щоб стати інтелектуальною власністю, вони мають одержати правову охорону: фізична (фізичні) особи подають заявку до патентного відомства — патентне відомство здійснює експертизу заявки, про що і видає відповідний документ, власне патент. *Сама інтелектуальна власність не є результатом інтелектуальної праці, вона являє собою виключні права на цей результат.* Захищати свою інтелектуальну власність (за законодавством будь-якої держави) від порушників (копіювання, підробки тощо) має сам патентовласник, він має

також виявляти зловмисників, відбувати (позивати) спір про несанкціоноване використання об'єкта охорони ІВ, на який видано патент. Також саме патентовласник може продати права на використання винаходу, уклавши ліцензійну (дозвільну) угоду. Тобто всі ці питання, не входять безпосередньо до сфери дії патентного відомства, тим більше як урядового органу державного управління. Через інформаційне забезпечення процесів комерціалізації результатів науково-технічної діяльності матеріалами фондів національної патентної документації (розділ 2.6, абз. 9 програми) система охорони об'єктів ІВ може лише сприяти патентовласникові при здійсненні ним операцій у відповідному секторі ринку.

У цьому контексті — щодо «комерціалізації результатів інтелектуальної діяльності» та «інформаційного забезпечення в сфері інтелектуальної власності» — зовсім не випадковими (або не продуманими) є положення програми щодо ролі та участі державних органів НТІ у процесі її реалізації.

Саме ці положення програми чітко окреслюють ті сфери, до яких патентні відомства мають опосередковане відношення, а саме:

1) щодо інфраструктури в сфері ІВ — «Держдепартамент ІВ має здійснювати керівництво формуванням та розвитком функціональної інфраструктури *державної* системи охорони ІВ, до якої ... мають увійти ... структурні підрозділи з питань ІВ, які мають бути утворені у складі... центрів НТЕІ» (розд. 2.2, абз. 6).

Держдепартамент є урядовим органом державного управління у складі Міністерства освіти і науки України, що саме по собі створює організаційну невизначеність. Центри НТІ, окремо кожний, підпорядковані тому ж міністерству, але на відміну від патентної сфери не утворюють організаційно-правового угруповання, тобто системного статусу ЦНТЕІ набули, так би мовити, історично. На сьогодні не існує ніякого законодавчо оформленого акта, який підтвердив би такий статус. Не можна також говорити про систему НТІ як національну за статусом, тобто не існує такого урядового рішення, яке визначало б відповідні дії держави щодо своєї (органи НТІ не підлягають приватизації) інформаційної інфраструктури;

2) «забезпечення подальшого формування фондів національної патентної документації в органах державної системи науко-

во-технічної інформації» (розд. 2.6 «Інформаційне забезпечення діяльності в сфері інтелектуальної власності з використанням сучасних інформаційних технологій», абз. 9).

Фонд національної патентної документації, безумовно, є однією із найвагоміших складових змістовного інформаційного ресурсу (ЗІР) держави за результатами науково-технічної діяльності. Формування такого фонду можливе виключно у межах тієї інфраструктури, яка створює передумови його формування — Українського інституту промислової власності, що належать до сфери управління Держпатенту. Формування фонду не є суто технічною процедурою — це складний науково-виробничий комплекс, а з огляду на відомості, які підлягають зберіганню, ще й неабияка проблема захисту (у тому числі технічного) таких відомостей. Крім того, матеріали фонду підлягають ще й аналітичному опрацюванню не тільки у процесі формування фонду, а й з огляду на інформаційно-аналітичне забезпечення управлінських та господарських структур різних рівнів та фахового спрямування. Тобто виникають ті самі питання, що й до попередньо викладеного положення програми, але до них ще додається і проблема власника фонду: якщо матеріали із Українського інституту промислової власності передаються (тут неістотно яким чином це технічно здійснюється) до визначеного ЦНТЕІ, то яка структура, якої відомчої підпорядкованості, надалі нестиме відповідальність за розміщення таких матеріалів у масиві автоматизованої системи, хто здійснюватиме обробку даних, надання їх у доступ, на чий рахунок підуть амортизаційні відрахування та яким чином здійснюватиметься оплата за надання інформаційного забезпечення користувачам за матеріалами фонду? А якщо до цих питань додати «створення» бірж об'єктів інтелектуальної власності (розд. 2.3 програми, абз. 7) та стимулювання ІВ (там само, абз. 8), стає взагалі незрозуміло, яким чином — у правовому та організаційному аспектах здійснюватиметься така діяльність щодо власників самих патентів.

Що ж до виробничої структури, яка порівняно швидко була відтворена у суверенній Україні, то слід сказати, що відбулася реорганізація системи охорони інтелектуальної власності у межах широкомасштабної адміністративної реформи. Згідно з По-

становою Кабінету Міністрів України у квітні 2000 року в складі Міністерства освіти і науки України створено Державний департамент інтелектуальної власності, який отримав статус органу державного управління. За наказом Міністерства освіти і науки у червні 2000 року були утворені підпорядковані Держдепартаменту державні підприємства — «Український інститут промислової власності» та «Українське агентство авторських та суміжних прав».

Отже, управління такою важливою для кожної держави сферою діяльності, як авторське право та суміжні права, а також охороною прав на об'єкти промислової власності в Україні здійснюється єдиним державним органом. Це й зумовлює значною мірою єдину і послідовну політику використання ЗІР з питань охорони інтелектуальної власності як у масштабах всієї держави, так і у процесах становлення України у світі.

Так, Державний департамент інтелектуальної власності доручив створення Української інтернет-біржі промислової власності утвореному у травні 2001 року Українському центру інноватики та патентно-інформаційних послуг. Концепція, яку розробила ця установа, основну увагу приділяє таким напрямкам функціонування біржі:

- інформування виробників продукції про вітчизняні та закордонні винаходи, що стосуються галузі їх діяльності;
- активне рекламування конкретних винаходів, корисних моделей, сортів рослин тощо на замовлення власників цих об'єктів;
- оприлюднення інформації про реальні успіхи в галузі інновацій в Україні.

При цьому мають бути створені інформаційно-довідкові масиви: 1) потенційних споживачів промислової власності (інноваторів); потенційних постачальників об'єктів промислової власності (науково-технічних установ, патентних повірених, окремих активних винахідників) в Україні; 2) нормативно-довідкових відомостей з питань охорони промислової власності в Україні, юридичних та фінансових аспектів інноваційної діяльності; 3) реєстру клієнтів — їх реквізити, сфера інтересів, статус, участь в операціях.

Головним результатом діяльності біржі має стати збільшення кількості укладених угод щодо використання об'єктів про-

мислової власності України у вітчизняному виробництві та за кордоном.

При розробці концепції інтернет-біржі та її реалізації особлива увага має бути приділена системі електронної сплати послуг, до якої входить: ознайомлення з переліком послуг та умовами їх надання, замовлення обраної послуги з визначеними умовами її надання, сплати за таку інформаційну послугу, отримання замовленої інформації електронною поштою. Для впровадження цієї моделі мають бути використані засоби безготівкової оплати товарів і послуг (інтернет-магазин), які нині зовсім не враховуються в документації фінансово-бухгалтерської звітності в Україні, але досить широко використовуються при веденні бізнесу за технологією Інтернет.

Зауважимо, що стратегія розвитку біржі об'єктів, зареєстрованих у системі охорони інтелектуальної власності, має бути глибоко продуманою і обґрунтованою. Вона не повинна бути зведеною до «електронного табло», а працювати на встановлення ціни, вибору конкурентної стратегії і, як наслідок, оптимального виду діяльності. Не випадково, а цілком закономірно у світі склалася практика функціонування ринків (що відтворено у відповідних біржах) — товарних, акцій, валютних, цінних паперів, сукупність яких утворює світову фінансову систему¹⁴⁹. Ці ринки виявляють конкурентоспроможність не «товарів», а промислових структур, у результаті роботи яких ці товари з'являються. Тобто існує проблема з неконкурентоспроможними промисловими або, узагальнюючи, виробничими структурами. Відомо, що розпочавшись з 1992 року, така функціональна реорганізація в Україні ще далека до завершення. Тому говорити про інтернет-біржу промислової власності можна лише в контексті вироблення, пошуку стратегії, яка забезпечила б розширення кола споживачів та, деякою мірою, надавала інформацію щодо раціонального використання промислових об'єктів.

Для процесів економічної трансформації суспільства, що відбуваються в Україні, характерною є зміна галузевої структури щодо створення об'єктів ІВ, які пропонуються на ринок. Зменшується частка науково-технічної продукції, яка могла б застосовуватися у базових галузях промисловості. Залишається невисокою активність іноземних заявників, що свідчить про малу

зацікавленість вкладати кошти в національний науково-технічний продукт.

Динаміка винахідницької діяльності¹⁵⁰ свідчить про її нестабільність у період з 1993 по 1999 роки. Найбільше її зростання спостерігалось у 1994 і 1997 роках з подальшим різким зниженням у 1995 і 1998 роках. Показовим є також і розподіл отримання патентів в Україні іноземними заявниками з 1993 по 1998 рік. Виявляється, що їх кількість тісно пов'язана з кількістю патентів, виданих національним заявникам, причому тенденція до її зростання чи зниження, як правило, чітко відповідає зацікавленості інвесторів до вкладання коштів в ту чи іншу галузь нашої економіки. У 1998 році кількість патентів, що отримали іноземні заявники, наблизилась до нижньої критичної позначки. Якщо брати до уваги, що у наступні роки ситуація не поліпшилася, навряд чи можна вести мову про оптимістичні наміри інвесторів. Серед галузей економіки найбільша винахідницька активність іноземних заявників спостерігається у хімічній промисловості, машинобудуванні та металургії — 74,4% від загальної кількості патентів, виданих в Україні за цей період. Водночас цей показник значно знизився стосовно таких галузей, як приладобудування, добувна, легка, медична, електроенергетична та інші. Майже не отримували патентів іноземні заявники у геології, водному та лісовому господарствах (менше 1 % загальної кількості).

Тобто винахідницька активність в Україні — сьогодні на низькому рівні (кількість виданих патентів за період з 1993 по 1998 роки в 40 разів менша, ніж у США, або приблизно у 8 разів менша в перерахунку на душу населення). Фактично вона ще нижча, якщо брати до уваги, що частка «сильних» патентів, виданих з проведенням експертизи, по суті, за цей період становить 23,2 %.

Одночасно зростає активність іноземних заявників на подання заявок на знаки для товарів та послуг, що свідчить про сприймання ними України як потенційного ринку збуту своїх звичайних товарів, але не інтелектуальних продуктів, які мали б сприяти зростанню економічного потенціалу України¹⁵¹. Така тенденція є досить тривалою у часі, й повільне зростання рівня пропозиції інтелектуальних продуктів одночасно із сталою тенденцією до спаду на попит викликало появу цілої низки кон-

цепцій, спрямованих на систему державного стимулювання щодо створення конкурентоспроможних передусім технічних об'єктів. Напрями цієї державної політики відбиті, зокрема, у Концепції створення державної системи розвитку і захисту «критичних технологій» (1994 рік), Національній програмі України «Критичні технології» (1994 рік), Концепції створення державної системи формування і реалізації технічної політики України (проект) (1995 рік), Концепції державної промислової політики України (1996 рік).

У всіх цих концепціях наголошувалось на створенні механізмів їхньої реалізації й у інформаційному аспекті. Як правило, це передбачало реалізацію інформаційного забезпечення на етапі передачі технологій, тобто після їх розробки, на стадії їх існування як кінцевого продукту у визначеній технічним завданням матеріальній формі. Здійснення інформаційного забезпечення ідеологічно передбачалось у традиційних формах надання підприємствам, організаціям, установам, підприємцям, державним органам влади та іншим суб'єктам інформації про технології, в яких вони зацікавлені, для встановлення контактів з розробниками та виробниками продукції (без попереднього виявлення попиту). Передбачалось також інформаційно-аналітичне забезпечення міжнародного науково-технічного співробітництва (без урахування механізму захисту інформації). А на таких етапах, як розробка технічного завдання, проведення техніко-економічного обґрунтування тощо витрати на здійснення інформаційного забезпечення, хоч би задля порівняння з існуючими зразками по галузі, в межах якої здійснюється розробка, навіть не передбачались¹⁵². Інформаційно-аналітичне регулювання міжнародного співробітництва у сфері державної науково-технічної та промислової політики передбачало створення Національного науково-інформаційного центру, який концентрував би зарубіжну НТІ та забезпечував її доступність на некомерційній основі¹⁵³, що не здійснено.

Усе це свідчить про слабку скоординованість цілей науково-технічної політики та загальних цілей розвитку нашої держави, що відбивається і на механізмі реалізації вже прийнятих законодавчих актів та функціонуванні відповідних складових СНІР, зокрема системи науково-технічної інформації України.

2.1.2. Науково-технічна інформація та система її організації

Структурно НТІ становить сукупність інформаційних органів, що постійно здійснюють інформаційну діяльність у визначеній галузі знань чи галузі виробництва й об'єднані в одну систему. За функціональними ознаками структурне об'єднання таких органів відбувається на засадах, що визначаються нормативно-правовими документами з питань одержання, обробки, зберігання, використання та поширення інформації за результатами науково-технічної діяльності в Україні (детальніше про це — п. 1.3).

Тому особливо показовою є ситуація, що склалася з реалізацією положень Закону України «Про науково-технічну інформацію»¹⁵⁴, прийнятого 25 червня 1993 року. Найбільш критичним є стан виконання ст.8 закону — «Визначення та склад національної системи науково-технічної інформації», п.3 — структура національної системи НТІ.

Діяльність з організаційно-правового забезпечення цих положень закону була розпочата наказом ДКНТП (першим попередником сучасного Міністерства освіти і науки України) від 29 липня 1995 року. Ним передбачалась робота з підготовки проєктів типових нормативних документів — положення про державні територіальні органи НТІ, галузеві та відомчі органи та служби НТІ, мережу науково-технічних бібліотек, які були передані до ДКНТП.

Тобто була наявність інфраструктури НТІ з цілком адекватною, як на той час, матеріально-технічною базою. Відчувалась потреба державної уваги до цієї системи, здійснення відповідних регуляторних заходів. Одночасно починалися розробки Програми забезпечення функціонування та розвитку національної системи науково-технічної інформації, яка визначила б порядок та стратегію дій у цій системі стосовно процесів трансформації суспільства.

На жаль, ці питання залишилися не вирішеними, а програма — так і не розробленою. Натомість систему НТІ почали поєднувати то з інформаційною політикою, то з напрямом охорони інтелектуальної власності, то з трансфером технологій. Такі намагання свідчать про одне: належний розвиток організаційно

оформленої інформаційної ланки у науково-технічній, промислово-виробничій, інноваційній політиці держави набуває ключового значення. Навіть при повному самоусуненні держави від розгляду цих питань не припиниться створення приватних баз та банків науково-технічної інформації, посередницьких фірм, які й будуть суттєво впливати на формування науково-технологічного, інвестиційного «клімату», а менеджмент перехопить роль державного управління, принаймні щодо визначення пріоритетних напрямів розвитку держави та прогнозування соціально-економічних наслідків їх реалізації.

Невиконання цього положення закону підтверджується і відсутністю будь-якого урядового рішення щодо ст. 18. «Державне управління в сфері науково-технічної інформації», текст якої наведемо повністю: «Кабінет Міністрів України визначає орган державного управління, який забезпечує організацію діяльності у сфері науково-технічної інформації, здійснює функціональне управління національною системою науково-технічної інформації, формує і реалізує політику в цій сфері». На сьогодні органом державного управління є Міністерство освіти і науки України, яке не має чітко визначеного внутрішнього структурного підрозділу щодо цієї сфери діяльності. Про це свідчать дані, наведені у доповіді першого заступника міністра освіти і науки України на колегії МОН 27 березня 2001 року: «Протягом 2000 року в УкрІНТЕІ та установах, що виконують роботи в рамках системи науково-технічної інформації, підготовлено понад 1,5 тисячі інформаційних продуктів, зокрема 100 наукових доповідей, 530 рефератів, 170 тематичних довідок тощо»¹⁵⁵. Ці всі роботи були виконані за умови держбюджетного фінансування діяльності довідково-інформаційних фондів. Але про діяльність самої системи, зокрема таких її структурних ланок, як центри НТЕІ, у доповіді взагалі не йшлося. Можна сказати¹⁵⁶, що основні рушійні сили радянського способу організації науково-технічної діяльності зникли, проте форми та інституції, які забезпечували такий спосіб організації науки та освіти, залишилися, але, додамо, регулятивна політика держави на рівні її реалізації урядовими виконавчими структурами є вкрай незадовільною.

Можна констатувати, що тільки відсутність державної підтримки науково-інформаційної діяльності, наявність якої

передбачена ст.17 закону, призвела до розпорошення та розкоординації цілеспрямованої фінансово-кредитної політики щодо розвитку системи державних інформаційних ресурсів з науково-технічного та виробничого доробку України, у тому числі невизначеності відповідної податкової політики щодо надання інформаційних продуктів та послуг споживачам, нормативно-методичної бази процесів надходження інформації до органів НТІ. Також відсутній встановлений на урядовому рівні Порядок передачі юридичними особами державним органам НТІ інформації про науково-технічні досягнення та виробничий досвід, що обумовлено ст. 10 закону.

Закон передбачає виконання в системі НТІ, через її структурні підрозділи, здійснення заходів, спрямованих на формування як ринку НТІ (розд. IV у цілому), так і ринкових відносин на інших сегментах. Це обумовлено положеннями статей 3, 7, які теж не набули відповідної дієвості. Проте у Законі України «Про оподаткування прибутку підприємств» ст.3 — плата за інформаційне та довідково-консультаційне обслуговування відноситься на собівартість продукції (послуг). Це тоді, коли немає навіть сучасного нормативного визначення такого обслуговування. Дуже добре розуміючи його цінність, приватні спеціалізовані підприємства, які діють чи не в усіх галузях державного господарювання, почали збирати відповідну НТІ, проводити прогнозно-аналітичні дослідження на конкретні замовлення та й просто продавати підбірки (часто реферативні) за тематикою.

Вивчення ринкових можливостей конкретних новацій стало однією із форм підтримки інноваційного бізнесу. У технопарках та великих промислових структурах для цього існують або створюються спеціальні служби, у тому числі й у кредитних установах з метою зменшення ризику інвестицій. Але здебільшого ці спеціалізовані служби використовують дані та відомості, що накопичуються у державних фондах відповідних змістовних інформаційних ресурсів.

Як зазначалося¹⁵⁷, інформаційний потік, спрямований на підприємців, має забезпечувати маркетингові дослідження попиту на наукові розробки, технологічні нововведення та інші інновації. Сюди ж відносять й інформацію про нові технології та їх можливості. Ця науково-технічна література здебільшого недоступна виробникам (особливо у сільськогосподарському

комплексі), а до патентних бібліотек вони звертаються лише тоді, коли виникає потреба перевірити власний винахід на патентну чистоту.

Відносно позитивна ситуація склалася з реалізацією положень ст.11 «Державна реєстрація, облік і використання результатів науково-технічної діяльності» цього закону, зокрема пунктів 1, 2. Постановами Кабінету Міністрів України¹⁵⁸ в Україні започаткована державна система реєстрації та обліку науково-дослідних, дослідно-конструкторських розробок та захищених дисертацій, створені також відповідні порядки обліку та реєстрації, здійснені заходи щодо функціонування такої системи в єдиному виробничому комплексі та за єдиною технологічною дисципліною. Але внаслідок відсутності цілеспрямованої політики з використання цього державного фонду його матеріали не використовуються навіть за прямим призначенням — при проведенні експертизи на відповідність проектів, що подаються за науково-технічними програмами. Також не провадиться робота зі створення звітів урядові у вигляді щорічних національних доповідей, де були б детально висвітлені та проаналізовані результати науково-технічних досліджень, у тому числі й у фінансовому аспекті, надані рекомендації (можливо, з експертним підтвердженням) щодо впровадження (трансферу, експорту тощо) окремих науково-технічних продуктів і обґрунтовані підстави щодо пріоритетності науково-технічного розвитку, який фінансується чи має фінансуватися державою.

Більш того, дія цих постанов не приведена у відповідність до постанови Кабінету України №412 від 3 червня 1993 року «Про систему науково-технічних програм»¹⁵⁸, якою також впроваджується єдина державна система реєстрації науково-технічних програм, проектів, що входять до її складу, виконавців таких проектів, а також проектів, що були подані на розгляд, але не пройшли конкурсу на відповідність визначеним програмам. Незважаючи на деяку відмінність цього процесу в сучасній формі порівняно з тим, що був започаткований, реєстрація залишилась майже в тому самому вигляді*. Удосконалення торк-

* Упорядкованість процесу реєстрації науково-технічних програм та узагальнення інформаційних матеріалів про хід їх виконання регулювались спільним наказом Держкомітету України з питань науки

нулись лише технічної системи та засобів обробки матеріалів, що подаються. Не можна не помітити однаковості, навіть ідентичності цих фондів. Перший — створюваний згідно з дією постанов № 162 та № 155, створюється в Українському інституті науково-технічної та економічної інформації (УкрІНТЕІ), і його матеріали є більш-менш доступними загальному споживачеві. Другий фонд (за постановою №412) створюється в ІАЦ Міністерства освіти і науки України і є практично недоступним. Ні разу не порівнювались матеріали фондів і не виконувались аналітичні роботи щодо ефективності впровадження чи маркетингової цінності поданих проектів, хоча б у фінансовому аспекті. Слід додати, що матеріали державного фонду УкрІНТЕІ не розповсюджуються у вигляді періодичних реферативних збірників за тематичними підрозділами фонду, бази даних лише частково працюють у промисловому режимі їх експлуатації.

Збір і аналіз інформації про хід реалізації програм за пріоритетним науково-технічним напрямом з одночасним відтворенням та аналізом інформації за зареєстрованими НДДКР по цих програмах мала б виконувати спеціально створена для цього установа — УкрІНТЕІ, із залученням ЦНТЕІ (як структурних елементів національної системи НТІ). Але регулярність надходження первинної інформації, правомочність центрів щодо відстеження реалізації розробок на кінцевому етапі, доступ до фонду ІАЦ МОН мають бути передбачені в нормативному акті, затвердженому хоча б на рівні Міністерства освіти і науки України.

За ст. 21 Закону «Про науково-технічну інформацію» Україна є учасницею Угоди про міждержавний обмін науково-технічною інформацією від 26 лютого 1992 року. У зв'язку з цим на УкрІНТЕІ рішенням уряду покладені функції Національного інформаційного центру, який має забезпечувати співробітництво України в такому обміні. Якщо нині міждержавна координаційна рада з НТІ увійшла до підрозділу МЕК, то це ще не

і технологій, Міністерства статистики України від 7 червня 1994 року №90/132 та постановою Кабінету Міністрів України від 1 вересня 1994 року № 609 «Про положення про координаційну раду з пріоритетного напрямку розвитку науки і техніки». Проте організаційна та фінансова невизначеність на рівні виконавчих структур не мала бажаного ефекту.

означає скасованості угоди. Але, починаючи з 1996 року, розробки тих програм (проектів), що забезпечували виконання угоди та були спрямовані на стратегію розвитку міждержавних відносин у сфері НТІ, не фінансувались міністерством. Зауважимо «у дужках», що фінансування цього напрямку робіт відбувалося вже через третій структурний підрозділ міністерства — управління з питань міжнародної діяльності. У результаті питання відкритого та рівноправного доступу громадян держав-партнерів за угодою до інформаційних ресурсів (НТІ) України, як і доступ громадян України до інформаційних ресурсів, обумовлених угодою країн, залишилося відкритим.

Розуміння важливості реального впливу наукових досліджень і розробок на розвиток економіки приводить до усвідомлення вагомості аналізу результативності науково-технічної політики, а відтак і до НТІ як підґрунтя прийняття управлінських рішень.

Традиційно до національної системи НТІ відносять¹⁶⁰: мережу наукових бібліотек (більше 1000), інформаційні підрозділи науково-дослідних установ (понад 200), ЦНТЕІ (18 разом з УкрІНТЕІ), деякі наукові заклади, що займаються питаннями автоматизованого процесу випуску тематичних реферативних наукових видань (Інститут проблем реєстрації інформації НАН України та Національна бібліотека України ім. В.І. Вернадського), а також організації та установи, які сприяють забезпеченню бібліотечним закладам доступу до світової періодики в електронному форматі. Але навіть і це існування розрізнених закладів, установ та організацій, діяльність яких деякою мірою відстежується та фінансово підтримується Міністерством освіти і науки України, НАН України, позабюджетними фондами та громадськими установами, органами місцевого самоврядування не відповідає основному положенню Закону України «Про науково-технічну інформацію»: «Національна система науково-технічної інформації — це організаційно-правова структура, за допомогою якої формується державна інформаційна політика, а також здійснюється координація робіт по створенню, користуванню, зберіганню та поширенню національних ресурсів науково-технічної інформації з урахуванням інтересів національної безпеки» (ст.8, п.1).

Такий стан справ призводить, зокрема, до відсутності достатньо авторитетних державних консалтингових агентств, які

могли б стати посередниками між інвестиційним джерелом та незавершеним (за різними причинами) об'єктом у вигляді привабливої для інвестора науково-технічної продукції. Це особливо відчутно для малого бізнесу, для окремих фізичних осіб, для незавершених (на рівні існування зразка) науково-технічних розробок. Те, що до системи НТІ не були включені фонди інформації, з яких був знятий гриф «секретно» (принаймні з 1992 року), призвело до того, що технологічні брокери інших країн скористались такою незахищеністю і недалекоглядністю, а Україна змушена або відновлювати попередні досягнення, або купувати готовий продукт, не фінансуючи власної науково-технічної діяльності.

Регуляторну функцію держави щодо установ НТІ відіграють окремі положення указів Президента України, зокрема¹⁶¹:

— «Про рішення Ради національної безпеки і оборони України від 17 червня 1997 року «Про стан науково-технічної сфери України та невідкладні заходи щодо підвищення ефективності її державного регулювання» від 13 жовтня 1997 року № 1147;

— «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 12 липня 1997 № 663;

— «Про рішення Ради національної безпеки і оборони України від 3 липня 2001 року «Про невідкладні заходи щодо виводу з кризового стану науково-технічної сфери України і створення реальних умов для переходу економіки на інноваційну модель розвитку» від 20 серпня 2001 року № 640;

— «Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України» від 6 грудня 2001 року № 1193.

У Російській Федерації факт наявності і дієздатності системи НТІ на рівні державної політики підтверджений постановою Уряду РФ від 24 липня 1997 року № 950 «Положення про систему науково-технічної інформації Російської Федерації»¹⁶². Однією із функцій системи визначено інформаційне забезпечення зовнішньоторговельної діяльності, зокрема, «відтворення та розвиток системи інформації про сучасні досягнення вітчизня-

ної та зарубіжної науки і техніки, передовий виробничий та підприємницький досвід з використанням можливостей науково-дослідних центрів, включаючи вищі освітні установи та російські закордонні установи», що у свою чергу визначено постановою Уряду РФ про федеральну програму розвитку експорту Російської Федерації від 8 лютого 1996 року № 123¹⁶³ та документами про використання результатів науково-технічної діяльності¹⁶⁴.

Адміністративно-організаційна невизначеність вітчизняних установ НТІ як системи зі статусом національної, ускладнює механізм аналізу оцінки і використання даних змістовного інформаційного ресурсу держави за результатами науково-технічної діяльності як товару, зводить до мінімуму участь державних установ у процесах обігу НТІ, а як наслідок — гальмує процес становлення і розвитку ринкових відносин й у інших сферах господарювання.

В умовах прагнення України до вступу до Світової організації торгівлі та Європейського Союзу актуальним залишається питання удосконалення організаційно-правового механізму функціонування та розвитку, а надто — адміністративного визначення національної системи НТІ України. Вирішення цього питання має відбуватись на урядовому рівні.

Проголошений Президентом України інноваційний напрям розвитку держави передбачає залучення до цього процесу всіх наукових, академічних та галузевих закладів, промислових підприємств, діяльність яких пов'язана з розробкою наукоємної конкурентоспроможної продукції, нових технологій, впровадження їх у вітчизняне виробництво та просування на внутрішньому і зовнішньому ринках.

Для виконання завдань управління державою і зважаючи на серйозність та значущість проблеми є *необхідним програмно визначитись щодо засад та напрямів роботи системи НТІ країни.*

Головною метою створення програми є організаційна, правова та фінансова державна підтримка функціонування та розвитку інформаційної інфраструктури держави, впровадження єдиної технологічної дисципліни при створенні національного інформаційного ресурсу за результатами науково-технічної діяльності в Україні та використання цього ресурсу на засадах

ринкових форм взаємодії власників інформаційних продуктів та виробників інформаційних послуг у галузі НТІ.

У програмі має бути відображений сучасний стан системи НТІ, зумовлений наявністю законодавчої бази, що регулює правові, економічні та організаційні відносини всіх учасників інформаційної діяльності. Сучасний стан системи НТІ також характеризується наявністю нових світових та вітчизняних інформаційних технологій, що забезпечують принципово новий рівень узагальнення даних, їх передачі, трансформації та сприйняття такої інформації, що є витягом з різних видів та форм інформаційних ресурсів, створюваних у суспільстві. Суттєво змінила процеси обробки та зберігання інформації поява масових електронних інформаційних продуктів на дешевих носіях великої ємності. Завдяки поширенню індивідуальних персональних комп'ютерів навіть окрема особа може мати кращий рівень інформаційного забезпечення, ніж скажімо великий НДІ з його бібліотекою, відділом НТІ та обчислювальним центром. Функціонування глобальних комп'ютерних мереж зумовило наявність світових програмно-технічних стандартів. Це у свою чергу призвело до того, що державні установи більше не мають монополії ні на технічні засоби, ні на спеціалізоване програмне забезпечення, ні на спеціальні канали зв'язку. Усе це призвело до докорінних змін у структурі попиту на НТІ.

Аналіз цього чинника доводить, що підвищення рентабельності виробництва, рівня конкурентоспроможності продукції простіше та дешевше досягти не шляхом впровадження нових технологій, а поліпшенням системи організації інформаційної інфраструктури та управлінням маркетинговою діяльністю, що також має бути враховано при розробці програми.

Чинником, який суттєво впливає на сучасний стан НС НТІ, є наявність світового ринку НТІ, характерною рисою якого є великий рівень інтеграції інформаційних ресурсів. Більш того, такий традиційний інформаційний продукт, як інформація з передового досвіду, що фактично нав'язувався споживачеві, тепер здебільшого має статус «комерційної таємниці». Тому, як свідчить досвід багатьох країн світу (передусім США, Великої Британії, Франції, країн Латинської Америки), саме на створення інформаційних продуктів має сенс спрямовувати державне фінансування. Подальші експлуатаційні витрати можуть

покриватися госпрозрахунковою діяльністю інформаційних установ. В Україні склалася ситуація, коли при формуванні вітчизняних та використанні закордонних баз і банків даних, виробник керується маркетинговими проробками, які здебільшого є його комерційною таємницею, а споживачеві надається вибір — або виконувати угоду, що нав'язується продуцентом, або шукати іншого фондвласника, який продасть свій продукт згідно з нормативними вимогами споживача. Прикладів останнього у світовому досвіді немає. Це положення свідчить, що до створення нормативних вимог треба підходити виважено з тим, щоб залучити до складу інтегрованого інформаційного ресурсу України і виробників інформаційної продукції недержавного сектору господарювання.

В Україні, як і в інших країнах СНД, але на відміну від Російської Федерації є ще одна проблема, пов'язана з формуванням єдиної державної системи інформаційних ресурсів. Це використання інформаційних матеріалів обмеженого доступу з урахуванням конверсії оборонного комплексу України. У розв'язанні проблем конверсії інформаційні ресурси відіграють особливу роль тому, що налагодження конверсійного виробництва тісно пов'язане з виявленням розроблених раніше науково-технічних об'єктів та технологій подвійного призначення, збиранням інформації про них та організацією їх використання з цивільною метою. За необхідності її розв'язання в межах національної системи НТІ слід узяти до уваги, що інформація про науково-технічні об'єкти містилася в закритих джерелах, які зберігалися у спецфондах, доступ до яких був обмежений. Самі ж ці спецфонди у вигляді організованої системи зберігання та доступу з ретроспективою щонайменше 20 років залишилися в РФ. Значну частину цього фонду становлять звіти підприємств «союзного» підпорядкування, що опинилися на територіях нинішніх суверенних держав. Це робить цей фонд особливо цінним за наявністю в ньому інформації з унікальних розробок, але водночас виникають і проблеми як правочинності її використання Російською Федерацією (особливо щодо зняття грифу секретності), так і в плані вирішення питань промислової власності. Більш того, навіть у наш час при захисті дисертацій з засекреченої тематики реферати депонованих в Україні рукописів направляються до опублікування у реферативних виданнях ВІМІ,

що досі є головним центром інформаційної інфраструктури галузей промисловості, пов'язаних з оборонним комплексом РФ.

Основними офіційними джерелами НТІ з обмеженим доступом є: звіти НДДКР; опис секретних винаходів спеціалістів оборонних галузей промисловості; статті та повідомлення за результатами закритих НДДКР, опубліковані у закритих науково-технічних збірниках; закриті дисертації спеціалістів оборонного комплексу.

На сьогодні в Україні існує тільки державна фіксація наявності НДДКР та дисертацій закритої тематики, тобто тільки сигнальна інформація. Ніяких інших державних інформаційних видань в Україні не існує, а спецфонди (у вигляді звітів) є власністю підприємства, що виконувало замовлені державою НДДКР з закритої тематики. При цьому розпорядниками спецфондів є керівники державних підприємств. Щодо підприємств, які підлягають приватизації, порядок подальшого використання спецфондів секретної тематики вирішують державні органи, до сфери управління яких належать ці підприємства. При цьому слід зауважити, що мають місце непоодинокі факти, коли спецфонди закритої тематики залишаються безплатним додатком до цілісного майнового комплексу, що приватизується, їх подальшу долю визначають нові власники цих підприємств.

Налагодження системи формування, обробки, зберігання результатів науково-технічної діяльності закритої тематики є першорядним завданням інформаційної політики держави при розробці програми функціонування та розвитку системи НТІ в Україні¹⁶⁵.

Національна система НТІ України має будуватись як інтегрована на основі національної комп'ютерної мережі територіально розподілених та відомчо підпорядкованих інформаційних і документальних фондів проблемно-орієнтованого спрямування, у тому числі у вигляді баз та банків даних, електронних каталогів провідних наукових і технічних державних установ, підприємств та організацій різних галузей господарювання з правом доступу та використання першоджерел інформації за відповідно укладеними угодами або схемою, яка має бути обґрунтована у Положенні про національну систему НТІ.

Координація і організаційно-методичне керівництво, формування інформаційного ресурсу галузі має покладатися на цент-

ральний орган системи інформаційного забезпечення галузі та інформаційно-аналітичний центр міністерства цієї ж галузі.

За органами НТІ, у тому числі регіональними, які нині (на 2002 рік) входять до інформаційної інфраструктури Міністерства освіти і науки України, має закріплюватись функція інформаційного забезпечення метаданими (фактографічними, адресово-довідковими) щодо поточного стану виконання науково-технічних робіт за будь-яким напрямом їх ведення в системі державного господарювання.

УкрІНТЕІ має стати Національним центром науково-технічної, у тому числі економічної, інформації, і виконувати весь комплекс робіт, пов'язаний з інформаційно-аналітичним забезпеченням управлінських та виконавчих органів держави, координацією створення розподілених інформаційних ресурсів, у тому числі за напрямками: рекомендації щодо визначення виконавців для спільних дослідницьких проектів; партнерства інститутів (галузевих та академічних); співробітництва з організаціями, які надають підтримку вітчизняним інституціям у вигляді забезпечення ноу-хау, навчання кадрів, сучасним устаткуванням та відповідною інфраструктурою.

Така організаційна упорядкованість державних органів НТІ має створити засади єдиного внутрішнього інформаційного простору України, орієнтованого на її інтеграцію у світовий інформаційний простір.

Організаційна структура національної системи НТІ затверджується відповідними урядовими постановами, розробка яких має бути виконана в межах єдиної науково-технічної програми за рахунок часткового фінансування тими міністерствами, що мають свої центри або служби НТІ та здійснюють інформаційну діяльність на постійній основі. *Метою такої програми є створення єдиного територіально розподіленого змістовного інформаційного ресурсу України як системи баз даних, що визначають соціально-економічний стан держави, її регіонів у різних сферах діяльності і становлять науковий та практичний інтерес для різних категорій споживачів, у тому числі й на світовому ринку. Дія програми має бути спрямована на існуючу інформаційну інфраструктуру, досягнення єдиної технологічної дисципліни при формуванні та веденні БД великого обсягу з активним*

використанням ринкових форм, взаємодії державних та підприємницьких структур.

Основними джерелами фінансування програми забезпечення та розвитку системи НТІ (у державному секторі) можуть бути:

- інноваційний фонд міністерства, у тому числі галузевого, за умови його участі в програмі створення єдиної державної системи НТІ;

- державний бюджет, кошти якого мають використовуватися на створення та підтримку матеріально-технічної бази державного сектору інформаційної індустрії (БД, БнД, бази метаданих — БмД, системи обміну НТІ, фонди першоджерел тощо);

- • власні кошти установи, тобто того органу НТІ, що входить до єдиної державної системи НТІ як продуцент певних інформаційних продуктів та послуг, але для їх створення не користується технічними засобами, технологією опрацювання інформації та інформаційними масивами, створеними за рахунок держбюджету;

- кошти, одержані за рахунок надання інформаційних послуг, тобто отримані у випадках, не обумовлених у попередньому положенні або за їх винятком;

- інші джерела фінансування, як правило, досягнуті за рахунок виконання двосторонніх взаємовигідних угод, у тому числі в межах міжнародних домовленостей.

Міністерство освіти і науки України, до інфраструктури якого входять державні органи НТІ, згруповані УкрІНТЕІ, має зосередити кошти, розпорошені в різних розділах кошторису витрат на науку, для їх цільового використання на становлення та підтримку системи НТІ.

Програма, з урахуванням пропозицій та зауважень, має передбачати такі *основні положення:*

- підпрограма (підрозділ) розробки і впровадження нормативно-правової бази функціонування НС НТІ;

- підпрограма формування змістовного інформаційного ресурсу за результатами науково-технічної діяльності;

- підпрограма використання (за попередньою оцінкою) новітніх інформаційних технологій, у тому числі маркетингового спрямування, для створення інформаційних продуктів і надання інформаційних послуг; '

1) підпрограма визначення і впровадження економічних та методичних засад інтеграції України у світовий інформаційний ринок — технічні, технологічні, інформаційні аспекти (ЗІР).

Підпрограма 1 має бути спрямована на формування та реалізацію політики у сфері використання інформації за результатами науково-технічної діяльності в Україні, з урахуванням положень чинного законодавства, зокрема, на розвиток Закону України «Про науково-технічну інформацію», а саме:

- розробка правових норм та науково-методичних матеріалів щодо формування інформаційних масивів за результатами вітчизняної науково-технічної діяльності;

- визначення конкретних форм підтримки з боку держави виробників інформаційної продукції, у тому числі недержавного сектору господарювання;

- розроблення правової бази та відпрацювання механізмів міждержавного обміну НТІ;

- створення пакета нормативних документів, що обумовлюють інформаційну політику держави за матеріалами науково-технічного доробку, зокрема засекреченої тематики, визначення правових засад передачі науково-технічних досягнень ОПК у цивільний сектор виробництва.

Підпрограма 2 має бути спрямована на:

- упорядкування наявної системи власників інформаційних фондів за проблемно-орієнтованою тематикою досліджень, у тому числі закритої тематики;

- розробку принципів єдиної технології комплектування фондів першоджерел для забезпечення інформаційної взаємодії за попередньо створеними галузевими та відомчими системами НТІ.

Основною метою *підпрограми 3* є розробка методів техніко-економічних досліджень щодо оцінки ефективності використання новітніх інформаційних технологій у діючій системі державних органів НТІ та підтримка матеріально-технічної бази НС НТІ.

Підпрограмою передбачається визначення та впровадження єдиної технології інформаційного обміну (принаймні всередині держави); виконання розробок щодо програмно-аналітичних засобів обробки та передачі даних, які значно підсилюють дію існуючих комп'ютерних мереж інформаційного обігу.

Основною метою *підпрограми 4* є виявлення можливостей та визначення шляхів створення внутрішнього єдиного інформаційного простору України за технологією Інтернет, а також відпрацювання методології внутрішнього маркетингу вітчизняної наукової та технологічної продукції за матеріалами виконаних досліджень.

З погляду на систему регіональних центрів НТЕІ видається реальним здійснення ними таких робіт у складі державної системи НТІ: формування фондів інформаційних ресурсів регіонів — бази та банки даних про науково-технічний доробок, найважливіші потреби підприємництва, збирання інформації та вивчення економічних та виробничих можливостей регіону, а також встановлення зв'язків щодо реалізації науково-технічної продукції та технологій на внутрішньому та зовнішньому ринках.

Концептуально НТІ має бути визначеною, усвідомленою та оціненою. Функціонування системи НТІ має бути визнаною як окрема галузь політики та політичного аналізу й усвідомлена велика користь НТІ з соціального, політичного, економічного та військового погляду на неї. Більш того, в результаті виконання емпіричної та теоретичної науково-дослідної роботи має бути оцінена роль отриманої інформації у процесі винахідництва у цілому та галузі передачі (трансферу) технологій зокрема.

2.1.3. Становлення системи трансферу технологій

У англійській мові слово «transfer» використовується або як іменник, або як дієслово. У першому випадку воно перекладається як перенесення, переміщення, у другому — як переносити, переміщати, переставляти. Спрощено під трансфером технологій слід розуміти переміщення технологій.

При переході до соціально орієнтованої економіки великого значення набуває просування технологій до виробничих підприємств. З 80-х років на Заході цей процес відомий як Technology and Information Transfer, що відповідає сучасному вітчизняному розумінню трансферу технологій (ТТ)¹⁶⁶. Трансфер технологій — це така передача технологій, яка оформляється шляхом укладення дво- або багатостороннього договору між фізичними та/або юридичними особами, яким встановлюють-

ся, змінюються або припиняються майнові права і обов'язки щодо технологій та/або їх об'єктів. При цьому об'єктом технології є складова технології, пов'язана з використанням технології і/або виготовленням продукції чи наданням послуг при застосуванні технології, щодо якої немає обмежень про передачу її для використання. До об'єктів технологій належать у тому числі результати наукових та науково-прикладних досліджень, об'єкти права інтелектуальної власності, ноу-хау, технологічне обладнання та його комплектуючі, перелік, порядок та послідовність виконання операцій технологічного процесу виробництва продукції.

Зазначимо, що механізм комерціалізації інтелектуальної власності (ІВ) — це дуже важке завдання і в країнах з розвинутими інституціями власності, тим більше в Україні. У провідних, технологічно розвинутих країнах світу створені можливості і всі умови передусім на законодавчому та організаційному рівнях — для використання наукових, технічних та інженерних ресурсів державної науково-дослідної системи у приватному секторі. Такими ресурсами є високопрофесійні кадри, новітні технології та техніка так само, як і устаткування та прилади, що раніше були абсолютно недоступними.

Термін «технологія» є, на думку провідних міжнародних експертів, настільки широким, що навіть не має загального визначення. Так, за словником Вебстера, під технологією розуміють будь-яку «прикладну науку» або «сукупність знань, які призначені для створення об'єктів для блага людини». У галузі науки технологія є практичним застосуванням знань, отриманих у результаті наукових досліджень. Серцевиною технології є її принципи і методи — так зване ноу-хау. Процес, який дає змогу використовувати знання, технологію або інформацію, отримані в одній організації з однією метою, в іншій організації з іншою метою, і є, за прийнятим визначенням, трансфером технологій (див. п. 1.1).

Для України цей процес визначається як комерціалізація результатів наукових розробок, створених у різних галузях, з послідовним розширенням поля діяльності. Тобто аж до створення спільно з закордонними компаніями чи за їх замовленнями нових технологій різноманітного, передусім промислового,

використання, участь як у стратегічних, фундаментальних, так і короткострокових (прикладних) науково-технічних виробничих проектах, які задовольняли б потреби сучасного міжнародного ринку. Такий стан безпосередньо відповідає і потребам розвитку вітчизняних економічних перетворень.

Що стосується самого механізму втілення ТТ у процес державного господарювання, то тут найбільш яскравим як за терміном впровадження, так і за ефективністю досягнутих результатів є досвід США.

До 1980 року в США діяло положення, згідно з яким усі результати наукових досліджень, що фінансувалися з бюджету, належали федеральному уряду. Як наслідок цього розробники науково-технічної продукції не були зацікавлені у впровадженні власних розробок, оскільки вони не отримували від цього дивідендів. Протягом згаданого періоду всі американські університети патентували лише близько 250 розробок щорічно. У 1980 році був прийнятий закон, згідно з яким уряд передав свої права на розробки їхнім авторам. Тепер розробники могли патентувати свої результати під власним ім'ям, отримуючи право на продаж патенту або ліцензії. Крім того, закон зобов'язав усі федеральні лабораторії створювати офіси трансферу технологій, надав податкові та інші пільги фірмам, які використовували інновації у виробництві, визначив, що «трансфер технологій є обов'язком усіх науковців та інженерів». Ефект був вражаючим. За рік кількість патентів зросла більш як у десять разів, а проданих ліцензій — у сотні.

Наступним кроком було видання цілої низки законів та указів Президента США (1980-1994 роки), які визначили, що:

- трансфер технологій є основою підтримки конкурентоспроможності американської економіки;
- оцінка якості роботи дослідницьких лабораторій при визначенні обсягів їх бюджетного фінансування залежність від кількості запатентованих розробок та проданих ліцензій;
- розроблені у військово-промисловому комплексі технології подвійного призначення мають «неодмінно впроваджуватись у цивільний сектор»;
- роялті, які отримують розробники у разі продажу ліцензії на належний їм патент, оподатковуються за пільговим тарифом або взагалі звільняються від податків;

— університети зобов'язані включити до своїх програм курси технологічної освіти, патентне право.

Як наслідок, у країні було створено і правове поле для функціонування системи ТТ, структура якої на сучасному етапі має такий вигляд.

У організаційному плані, тобто органами держави, обов'язком яких є реалізація ТТ, стали офіси ТТ (ОТТ). Вони були створені при усіх університетах, лабораторіях, дослідницьких центрах США. Функціонують вони також при Національному науковому фонді, НАСА, Національному інституті здоров'я, міністерствах оборони, енергетики, сільського господарства, торгівлі тощо. Держдепартамент США надає офісам ТТ допомогу в співробітництві з аналогічними агентствами інших країн, готує відповідні міждержавні угоди. *На чолі системи стоїть Національне агентство з трансферу технологій разом з потужним Національним інформаційним центром, що підпорядковані Департаменту торгівлі США.* Створені при кожному ОТТ комп'ютерні бази даних дають змогу споживачам оперативно отримувати інформацію щодо існуючих розробок і навіть замовляти необхідну технологію у розробників. Особлива увага уряду приділяється трансферу оборонних технологій у цивільну промисловість.

Аналогічні системи трансферу технологій існують у Канаді, Німеччині, Великій Британії, Франції, Японії. На міжнародному ринку діють також відповідні агентства, які покривають цілі регіони, наприклад Агентство з трансферу технологій Далекого Сходу та Тихоокеанського регіону. В Ізраїлі також кожний університет має ОТТ, які займаються продажем технологій як всередині країни, так і за кордон. У Росії вже існує створена за західним зразком компанія «Російські технології», а також ряд підприємств, у тому числі спільних із США, які займаються трансфером технологій з країн колишнього СРСР на Захід.

Потрібно зауважити, що спостерігається значне відставання як у розумінні власне ТТ, так і відповідно до розуміння у засобах та заходах щодо його здійснення. У релізах геополітики «Глобальна інформаційна інфраструктура», яка стає особливо активною з 1996 року і до проведення якої приєдналась більшість країн світу, відзначається, що єдиним гальмом є узвичаєна недовіра до розвинутих країн. Зламати таку недовіру

стало завданням нової геополітики «Глобальне інформаційне суспільство»¹⁶⁷.

З такого погляду система трансферу високих технологій як підґрунтя подальшої інтеграції світового ринку, передусім інтелектуальної власності, пов'язана багатьма аспектами державного регулювання, принципами захисту інтелектуальної власності, авторського права, патентів, торговельних марок; секретністю і захистом інформації; телекомунікаційними інфраструктурами та технічними стандартами, оподаткуванням та митними тарифами. Тобто йдеться про розв'язання локальних проблем на засадах гармонізації національних політик, що узгоджуються за напрямками міжнародної інтеграції.

У суто прагматичному аспекті комерціалізація результатів науково-технічної діяльності базується на традиційних підходах, що відтворюють кон'юнктуру та попит на ринку товарів і послуг у цілому або в будь-якому з його секторів. Слід зазначити, що вивчення досвіду створення механізму комерціалізації результатів науково-технічної діяльності, зокрема у Російській Федерації, засвідчило, наскільки складним є вирішення цього завдання і з погляду створення відповідної нормативно-правової бази, і з суто організаційного. Ця робота потребує безпосередньої участі зацікавлених міністерств і відомств, узгоджених дій виконавчої та законодавчої гілок влади, значних витрат часу та зусиль для удосконалення організації такої роботи і накопичення та впровадження досвіду цієї діяльності.

Власне процес трансферу технологій за кордоном включає такі кроки:

- оприлюднення нової розробки, оскільки публікація результатів досліджень до подання заявки на патент робить їх непатентоспроможними; під «оприлюдненням» можна розуміти подання спеціальної заявки до відповідної організації, типу ОТТ, яка з'ясовує чи може ця розробка бути запатентована;

- у разі позитивної відповіді ОТТ допомагає розробнику оформити всі необхідні документи для патентування;

- одночасно ОТТ починає пошук потенційних споживачів цієї розробки;

- після видачі патенту ОТТ проводить переговори між розробником та споживачами щодо продажу патенту або ліцензії, розподілу роялті тощо;

— здійснює продаж патенту або ліцензії на конкурсних засадах.

Але нині, надаючи національні ноу-хау чи дослідні зразки зарубіжним компаніям внаслідок одноразової участі в зарубіжному чи міжнародному проекті або через контрактні умови одноразового гранту, Україна *позбавляє себе* можливості участі в реалізації результатів проекту на ринку у вигляді масового продукту. Такою ситуацією відсутності відповідного правового захисту інтересів як держави, так і окремих розробників користуються різноманітні закордонні фонди, корпорації, спільні центри.

Спільним для держав СНД є погляд на об'єкти ІВ як на результат науково-технічної діяльності, що існує у двох видах (див. п. 1.1):

— матеріальному — кінцеві продукти чи об'єкти науково-дослідних розробок, теоретичних досліджень внаслідок їх «матеріалізації»;

— інформаційному — опис об'єкта, способів його використання, методології (у фундаментальних дослідженнях), технології виробництва або застосування (технологія — часто отожднюється з ноу-хау).

За галузевого способу ведення господарювання питання впровадження, купівлі-продажу (особливо при виконанні міжнародних угод), трансферу, експорту об'єктів ІВ вирішуються в межах того відомства, що профінансувало відповідну науково-дослідну розробку (НДДКР) чи дослідження. Тим самим створюються передумови впровадження цими відомствами монопольної політики, оскільки кожне галузеве відомство в цілому можна розглядати як великий та потужний концерн.

При цьому положення Закону України «Про обмеження монополізму та недопущення недобросовісної конкуренції у підприємницькій діяльності» від 18 лютого 1998 року не поширюються на відносини, що виникають із прав на об'єкти ІВ. Це тим важливіше нині, коли особливо зростає економічна вагомість незапатентованої технічної продукції.

Крім того, різноманітність видів науково-технічної продукції, що створюється в Україні в цей час, джерел фінансування наукових досліджень, відмінності правових режимів завершених робіт та вплив ще цілого ряду інших факторів зумовлюють у

свою чергу різноманітність правових форм стосовно угод, що є чинними у сфері науково-технічної діяльності.

Із змінами інституту власності як такого в державі вперше виникли проблеми інтелектуальної власності (ІВ) на об'єкти, що мають відповідні ознаки. У СРСР ІВ у фінансово-господарському обігу практично не враховувалась як нематеріальний актив чи як об'єкт ринкових відносин. Її продаж за кордон здійснювався елітарними установами зовнішньоторговельної спрямованості. Торгові палати, навіть на концептуальному рівні, не були пристосовані до обслуговування тисяч і тисяч підприємств, не говорячи вже про науково-дослідні установи з їх великим творчим доробком.

У результаті все, що не належало до складу «промислових зразків» і, відповідно, не було захищене патентним правом, є нині змістовним інформаційним масивом держави. Цей масив є у своїй сукупності об'єктом ІВ і підлягає веденню, охороні та розпорядженню ним державними органами, але вже функціонального спрямування.

В Україні питання державних ресурсів науково-технічної інформації, яка є підґрунтям ТТ, стосовно об'єктів ІВ, створених до 1991 року, ускладнюється й тим, що правонаступницею СРСР є де-факто Російська Федерація. Це підтверджується відповідними положеннями російського законодавства та стратегічного підходу РФ при визначенні механізму державного регулювання процесу впровадження та комерціалізації наукоємної продукції і технологій:

— «Вся наукоємна продукція, створена за рахунок бюджетних коштів, у тому числі і за час існування СРСР, належить державі» (Указ Президента РФ «Про державну політику з введення в державний обіг результатів науково-технічної діяльності та об'єктів промислової власності у сфері науки і технологій» від 22 липня 1998 року № 863, п.2, абз. 3).

Питання стосовно порядку, обміну тощо фондів НТІ відкритої тематики, у тому числі й ті, що становлять ресурси спільного користування для країн СНД, розглядалися, обговорювалися та вирішувалися в межах галузевої міждержавної структури МНТР. Спеціалізованих організацій відповідного характеру щодо НТІ закритої тематики не існує в Україні навіть на рівні міжгалузевого інформаційного обігу. Державна реєстрація інформацій-

них об'єктів ІВ як ознака надання права на цей об'єкт (за аналогією з патентним правом) відбувається за порядком, започаткованим двома постановами Кабінету Міністрів України: відкритої тематики — за постановою від 31 березня 1992 року № 162, закритої — за постановою від 10 березня 1994 року № 155. Крім того, існує окремий Порядок щодо реєстрації інформаційних об'єктів інтелектуальної власності, виконаних на замовлення СБ України. Організаційно реєстрація провадиться УкрІНТЕІ Міністерства освіти і науки України. Довідка, що видається в УкрІНТЕІ юридичній або фізичній особі, є підставою для звільнення розробників-виконавців державних науково-технічних замовлень від ПДВ. Реєстрацію алгоритмів і програм покладено на УНЦ «Софт-рейтинг» МОН України (Положення, затверджене постановою КМ України від 18 липня 1995 року № 532)¹⁶⁸.

З аналізу ситуації випливає, що матеріальні та інформаційні види об'єктів інтелектуальної діяльності нерозривно пов'язані у процесі створення таких об'єктів. Найбільш неопрацьованим є питання використання змістовного інформаційного ресурсу за розробками закритої тематики, тобто технологій військового та подвійного призначення, що має вирішуватись як на міждержавному, так і на міжгалузевому рівнях.

Комплексне забезпечення заходів, яких потребує передача технологій, неможливо і недоцільно здійснювати тільки за рахунок коштів держави та силами тільки державних установ, враховуючи проблеми в економіці країни/Держава не може взяти на себе весь інноваційний ризик, а установи, що є власниками науково-технічних розробок, не в змозі охопити всі політичні та економічні аспекти в цьому питанні. Тому постають нагальні проблеми:

- сформулювати атрибути внутрішнього ринку технологій та наукових розробок;

- виробити правила роботи на цьому ринку для комерційних посередників та виступити з рядом законодавчих ініціатив, які мають привести у відповідність до цих досліджень чинне законодавство;

- комерціалізувати ринок наукоємних технологій з метою створення сприятливих умов для їх проникнення на зарубіжний ринок, зокрема, впровадити інститут венчурного капіталу.

254

Оскільки всі ці питання є системними, основну організаційну роль може відігравати спеціально визначений орган, який би врегулював: трансфер технологій на внутрішньому та зовнішньому ринках; пов'язану з цим фінансово-кредитну, податкову та інвестиційну політику держави; ліцензування посередницької діяльності у науково-технічній сфері, у тому числі й торгівлю НТІ; питання права на інтелектуальну власність, передусім на такі об'єкти ІВ, які не підпадають під патентну охорону.

При цьому мають бути відпрацьовані різні схеми надання технологій як об'єктів інтелектуальної власності (ІВ), наприклад:

- за виконанням спільного проекту. За світовою практикою цей варіант передбачає захист ІВ у межах проекту терміном на 5 років, коли головна організація-виконавець зацікавлена у найскорішому доведенні технології до кінцевого продукту. Організація впровадження може відбуватись за схемою: замовник НДДКР — держава, виконавець — юридична особа, впроваджувач (користувач) — приватна (комерційна) промислова структура;

- промислові структури визначають технології, в розробці чи закупівлі яких вони зацікавлені — передусім серед вітчизняних науковців — фізичних чи юридичних осіб. У цьому випадку організаційна структура ТТ виступає посередником між науково-освітніми установами, де провадяться основні фундаментальні стратегічні розробки з замовленого напряму, та промисловістю, що комерціалізує такі новітні технології. Цей спосіб потребує ліцензійного захисту через можливу довгостроковість впровадження;

- за посередництва визначеної ланки ТТ держава (зацікавлені відомства) «викуповує» результати НДДКР, що були створені за державні кошти, але не впроваджені своєчасно чи в повному обсязі, однак не втратили свого значення й доцільності на момент запиту. У цьому разі захист ІВ має визначатись за умовами контракту на впровадження;

- якщо промислові та комерційні структури (наприклад, у межах УСПП) дійшли згоди щодо проведення НДДКР, яка потребує значного часу, великих вкладень, пов'язана з високим ступенем ризику, але є стратегічно вигідною, партнером у проведенні таких робіт має виступати держава, а права на резуль-

тати виконання підлягають особливо ретельному визначенню щодо інтелектуального та матеріального внеску їх учасників.

При цьому спеціальна структура (установа) ТТ уповноважується здійснювати разом з податковими органами експертизу впроваджених інновацій та надавати офіційне рішення щодо застосування пільгових ставок податків.

Серед адміністративних заходів щодо ТТ можуть бути закони, укази Президента або постанови уряду, які вирішуватимуть питання технологічного розвитку окремих галузей, чи впровадження окремих технологій загальнонаціонального значення. (Яскравий приклад: свого часу, коли був відкритий транзистор, електронна промисловість США була орієнтована на випуск електронних ламп і виробів на їх основі. Тоді Конгрес прийняв Закон «Про об'єм запаяного вакууму», згідно з яким продукція цих компаній оподатковувалась відповідно до об'єму вакууму, запаяного у лампи. Наслідком цього закону став блискавичний перехід на напівпровідникову елементну базу). Роль установи ТТ у цій схемі — це відстеження появи таких революційних технологій та ініціювання прийняття адміністративних рішень щодо їх впровадження¹⁶⁹.

Ключовим питанням у наведених схемах є процес експертизи й аналізу інновацій. Він може бути забезпечений через регіональні або галузеві компанії з трансферу технологій, які працюватимуть на спеціальну державну структуру ТТ, або через систему головних інститутів, яка існувала колись у СРСР, а нині просто знищена.

Національна система НТІ і у разі організованості системи трансферу технологій України також виступає її інформаційним підґрунтям, як і у випадку використання змістовного інформаційного ресурсу — НТІ та її виробничої інфраструктури, на користь системи охорони інтелектуальної власності.

У системі НТІ України сьогодні, за відсутності цілеспрямованої інформаційної політики, 18 регіональних ЦНТЕІ ще якимось гуртуються навколо УкрІНТЕІ чи Міністерства освіти і науки України, зате у недержавному секторі господарювання діє маса «інформаційних компаній». Діапазон їх форм — від таких, що працюють на безприбуткових засадах, як правило, за закордонними субсидіями, до таких, що надають комерційну і довідкову, так звану економічну, інформацію, використовуючи для

цього інформаційні джерела на засадах особистої домовленості з працівниками державних фондів потрібного видового чи тематичного спрямування. Оформлення центрів другого типу мало б відбуватися за ліцензіями. Але, оскільки перелік видів ліцензійної діяльності й у 2000 році не містив такого окремого виду, як створення інформаційних продуктів та надання інформаційних послуг (не в сфері ЗМІ або реклами), право на цю діяльність надають просто органи місцевого самоврядування, що для власників компаній має певний сенс — *невизначеність щодо системи оподаткування (за відсутністю кінцевого продукту)*.

Отже, адміністративно-організаційна невизначеність щодо системи НТІ в Україні додатково ускладнює механізм використання інформаційного виду об'єктів ІВ, не відповідає реалізації світового принципу комерціалізації та надання результатів науково-технічної діяльності Technology and Information Transfer, зводить до мінімуму участь державних наукових установ у процесах торгівлі (обміну) інформацією, а як наслідок — інвестування та виробничої кооперації.

З погляду на сучасну мережу регіональних ЦНТЕІ та УкрІНТЕІ як на систему видається реальною її участь у трансфері технологій за такими напрямками (на відміну від її задіяності у державній системі охорони ІВ):

- формування фондів інформаційних ресурсів регіонів — бази та банки даних про науково-технологічний доробок, найважливіші потреби підприємництва, збирання інформації та вивчення економічних та виробничих можливостей регіону, а також встановлення ділових зв'язків щодо реалізації об'єктів ІВ на внутрішньому та зовнішньому ринках (країни СНД). Слід зауважити, що така спрямованість є характерною для ЦНТЕІ і нині, але вона стосується випадкових і нечисленних замовників. Переважно збирається та надається бізнес-інформація, а як посередники, при укладанні комерційних угод, ЦНТЕІ виступають переважно у неофіційній ролі, що створює сприятливі умови для некоректної діяльності. До того ж ЦНТЕІ входять до списку підприємств (об'єктів), що не підлягають приватизації;

- постійне вивчення інформаційних потреб підприємств різного рівня та форм власності щодо здійснення їх виробничої діяльності; міжрегіональний обмін такими даними; підтримка зворотного зв'язку підприємств та інформаційних органів.

Необхідність створення системи трансферу технологій державного рівня, що здійснює всі необхідні заходи з трансферу українських технологій за кордон та всередині країни, використовуючи для цього інформаційну інфраструктуру НТІ держави, доцільна й з погляду інформаційної безпеки.

Так, у США, ще за часів Р. Рейгана, була впроваджена політика посилення жорсткості щодо контролю при наданні технологій. По суті, ставилося питання про захист прав на інформацію, а не тільки про захист самої інформації (автоматизовані системи передачі даних, носії інформації тощо). Був прийнятий ряд нормативно-правових документів, що визначали предмет контролю, правила отримання дозволів та відповідальність за несанкціоноване надання технічної чи технологічної інформації іншим країнам.

Треба враховувати, що в часи фінансової скрути, надто повільного процесу практичної комерціалізації результатів науково-технічної діяльності, відсутності досвіду правового захисту інтересів держави і українських науковців на внутрішньому і міжнародному ринках інтелектуальної власності — централізованість та адміністративно-організаційна впорядкованість є нагальною державною потребою.

Докорінна зміна ситуації в науково-технологічній сфері держави можлива лише за умови впровадження системи скоординованих заходів із забезпечення дотримання вимог існуючих нормативно-правових актів, що регулюють питання функціонування вітчизняної науки, подальшого вдосконалення законодавства і системи управління наукою, вжиття практичних заходів щодо створення сприятливих умов для якнайширшого використання власного науково-технічного потенціалу для розвитку і технологічного оновлення вітчизняного виробництва, утвердження в суспільстві інноваційної ідеології, розуміння винятково важливого значення інформаційної складової та її захисту для сучасного і майбутнього України.

2.2. ПРАВО ВОЛОДІННЯ І РОЗПОРЯДЖЕННЯ ЗМІСТОВИМ ІНФОРМАЦІЙНИМ РЕСУРСОМ ЗА НАУКОВО- ТЕХНІЧНИМ ДОРОБКОМ В УМОВАХ РЕСТРУКТУРИЗАЦІЇ ВЛАСНОСТІ

Розвиток правового регулювання відносин, пов'язаних з формуванням та використанням інформаційних ресурсів та процесів, визначив орієнтацію на регулювання відносин у такій галузі, яка не була традиційно сферою права.

Новий погляд на інформацію як на ресурс та об'єкт матеріальної і інтелектуальної власності став поштовхом до вивчення специфічних особливостей та юридичних властивостей інформації, які багато в чому визначають і суспільні відносини, що виникають з приводу її використання та узгодження правового статусу.

Останнім часом поняття «інформаційного права» використовується різними спеціалістами з різних позицій, що, як зазначалося, впливає із самого предмета правових відносин інформаційного ресурсу.

Наприклад, «інформаційно-комп'ютерне право», «інформаційне право» досить часто стають темою обговорення не тільки на сторінках спеціальних наукових видань¹⁷⁰, а й у галузях, для яких інформація є визначальним фактором діяльності¹⁷¹. Так, у широкому розумінні інформаційно-комп'ютерне право розглядається як поєднання суспільних відносин, що становлять «інформаційне право» та «комп'ютерне право», а у вузькому — як здобуток цих множин. «Інформаційне право» відносять і до публічного права. Тобто маються на увазі інформаційні відносини як предмет правового регулювання, до чого залучені: суб'єкти інформаційних відносин, правовий режим отримання, передачі, зберігання і використання інформації, юридичні режими інформації різного виду, користування базами та банками даних, інформаційні правовідносини, відповідальність. Деякі автори пропонують визначити цей термін як систему соціальних норм і відносин, що охороняються силою держави та виникають у інформаційній сфері, — сфері виробництва, перетворення та споживання інформації¹⁷². Основними об'єктами правового регулювання тоді виступають інформаційні відносини, тобто відносини, що виникають при здійсненні інформацій-

них процесів: утворення, збирання, обробки, накопичування, зберігання, пошуку, поширення та споживання інформації. Інформаційне право визначається також як сукупність юридичних норм та інститутів, що регулюють інформаційні відносини у інформаційній сфері.

Правознавцям відомо, що серед соціологічних правових концепцій особливе місце посідає інституціоналізм, основи якого були закладені відомим французьким адміністратором Морісом Оріу (1856 — 1929), котрий теорію інститутів розглядав як єдність політичної та правової теорії, яка досягалася завдяки тому, що обидві вони базувалися на єдиному понятті інституту — діючого комплексу впорядкованих відносин, що виступає як єдність об'єктивного і суб'єктивного, що норми права створюються інститутами як автономними соціальними утвореннями (державою, торговими товариствами, профспілками тощо). Як обґрунтовує Е. М. Воротилін, саме інститути породжують норми права, але не норми права — інститути, а існування данного виду правових норм пояснюється необхідністю примусового регулювання відносин у соціальних колективах, що інститут містить потрібний нормативний потенціал: він є тривале існування плюс організація влади та консенсус¹⁷³.

Відповідно до теорії конституційного права України «інститути — це блоки, які охоплюють ту чи іншу сферу конституційно-правових відносин: інститут конституційного ладу, прав і свобод громадян, територіальної організації країни, принципів діяльності державних органів тощо. їм притаманний особливий механізм реалізації, де поряд із звичайними нормами конституції велику роль відіграють інші нетипові приписи, практика, взаємозв'язки з іншими, в тому числі галузевими інститутами»¹⁷⁴.

В Україні зроблені лише перші кроки до наукового осмислення на основі інститутів Конституції нового галузевого інституту права — інформаційного. У державних органах і серед наукової громадськості підтримана ідея кодифікації інформаційного законодавства. Розроблено й у жовтні 2000 року рішенням урядової комісії з питань інформаційно-аналітичного забезпечення органів виконавчої влади прийнято за основу проект Концепції реформування законодавства України у сфері суспільних інфор-

маційних відносин. На державному рівні виникла потреба юридично визначитися в найбільш важливих правових нормах поведінки їх учасників. Водночас це зумовило необхідність виокремлення та фіксування в державному управлінні напряму (інституції), що визначається як державне управління у галузі суспільних інформаційних відносин. Метою реформування інформаційного законодавства є втілення в життя державної політики в умовах розвитку суспільних інформаційних відносин в Україні: методів і засобів створення інформаційних ресурсів; їх обігу; збирання, накопичення, систематизації, використання і захисту.

Правовою основою формування, поширення, використання і захисту ЗІР та прав об'єктів на цю інформацію є правовий режим інформації.

У монографії НІСД «Інформаційні ресурси України: проблеми державного управління»¹⁷⁵ всебічно обґрунтовані основи правового режиму інформаційних ресурсів. Згідно з висновками авторів це встановлені законодавством правові норми регулювання суспільних інформаційних відносин щодо впровадження ступенів відкритості (закритості) інформації, порядку і правил віднесення відомостей до категорії обмеженого доступу, забезпечення режиму секретності (конфіденційності) гарантування права власності на інформацію та правового захисту інтересів суб'єктів інформаційної діяльності.

Змістовну сутність правового режиму інформації та його практичне застосування в системі суспільних відносин, пов'язаних із інформаційними ресурсами, розглянемо у п. 3.2. При цьому доцільно підкреслити лише такі аспекти: лише на основі правового режиму інформації можна встановити необхідний баланс між потребою у вільному обміні інформацією і допустимими обмеженнями на її поширення в інтересах національної безпеки та іншої суспільної необхідності; тільки правовий режим інформації є основою для встановлення режиму доступу інших держав до інформаційних ресурсів України та важливою умовою забезпечення їх рівноправного використання в процесі міжнародного інформаційного співробітництва. Тобто правовий режим інформації диктує всім суб'єктам інформаційних відносин правила поведінки із певним видом інформаційних ресурсів.

Розглянемо питання використання інформаційного ресурсу відповідно до його правового режиму в умовах реструктуризації власності та інформаційного ринку.

Власне інформація є нематеріальною категорією, і продають не інформацію, а право на її використання¹⁷⁶. Інформацію не можна прирівнювати до інформаційних видань, баз даних тощо, тобто до інформаційних продуктів і послуг, які мають усі властивості та ознаки товару і підлягають законам товарного виробництва та ринку.

Сучасну модель міжнародного використання змістовного інформаційного ресурсу можна умовно назвати виробничо-інвестиційною на відміну від раніше прийнятої торговельно-посередницької. Такий спосіб використання ЗІР у світі отримав назву міжнародного маркетингу, який дедалі частіше тепер розглядають як такий, що виходить за міжнаціональні рамки, як глобальний. Міжнародний маркетинг поширюється не тільки на власне торговельні операції, а й на інші сфери зовнішньоекономічних зв'язків: створення спільних та дочірніх підприємств, науково-технічний обмін, передачу ліцензій та ноу-хау, міжнародні орендні операції тощо.

З посиленням взаємозалежності та взаємозумовленості окремих національних ринків вони вже сприймаються не як окремі елементи, а дедалі частіше як єдиний універсум. За виробничо-інвестиційною моделлю взаємодій у світовому господарстві вже йдеться про існування на ринку окремих структурних блоків, а не певних товарів чи послуг¹⁷⁷.

Тому ЗІР — це об'єкт багатофункціональний, він створюється та споживається, по суті, в усіх сферах діяльності та має забезпечувати в сучасних умовах вирішення багатьох завдань, що стоять перед найрізноманітнішими його користувачами — органами державної влади, місцевого самоврядування, фізичними та юридичними особами.

Також маємо нагадати, що ЗІР може одночасно, поза вказаним функціональним навантаженням, виступати і як товар. Наприклад, предметом обміну, продажу, купівлі, трансферу є ЗІР, який містить відомості про корисні копалини, науковий та технічний стан розвитку суспільства, творчий потенціал тощо.

Звідси виникає юридична властивість змістовної інформації виступати як об'єкт, що передається від одного суб'єкта взає-

мовідносин до іншого, що потребує юридичного закріплення факту його належності суб'єктам — учасникам таких ділових (або інших) обігів.

Відносини власності як такі являють собою синтез матеріального змісту і вольового опосередкування. Саме тому цивілістичною доктриною визнається, що економічні відносини власності є водночас вольовими та невольовими. Невольовими вони є тому, що в умовах існування суспільства — об'єктивовані, тобто існують (у певних межах) незалежно від волі людей: люди не можуть жити, не вступаючи у відносини власності. Водночас ці зазначені відносини є вольовими, оскільки без цілеспрямованих, вольових дій людей виникати не можуть. Саме в силу наявності в них вольового елемента відносини власності можуть бути об'єктом правового регулювання¹⁷⁸.

Стосовно права власності здійснення права на свій розсуд, у тому числі й розпорядження ним, означає, що влада (воля) власника спирається безпосередньо на закон, існує незалежно від волі всіх інших осіб щодо цієї ж речі. Волевиявлення всіх інших осіб не лише спирається на закон, а й залежить від волі власника, зумовлене нею¹⁷⁹.

З цього погляду, коли в процесі трансформування загально-го суспільно-економічного порядку насамперед перебудовуються відносини власності, створення передумов для наповнення поняття змістовних інформаційних ресурсів, у тому числі НТІ, новим економічним змістом і послідовна його реалізація у господарській практиці є найскладнішим і водночас вирішальним кроком у процесі соціально-економічних перетворень. Політико-юридичне оформлення нових відносин передбачає й відповідальне реальне економічне будівництво суспільних відносин. Це більш тривалий етап глибинних перетворень суспільства, практичного розвитку і освоєння нового господарського механізму, який на ділі має довести свою прогресивність, здатність до виходу на вищий рівень соціально-економічної ефективності суспільного виробництва.

Як матеріальний об'єкт правовідносин ЗІР НТІ підпадає під застосування юридичних категорій користування та розпорядження.

Право користування¹⁸⁰ — це юридично закріплена можливість господарського використання майна та вилучення з нього ко-

рисних властивостей власником чи уповноваженими ним особами. Користування майном тісно пов'язане із володінням, яке є первинним для користування, хоча і здійснюються вони одночасно. Водночас право користування може здійснюватись і без права володіння (наприклад, користування даними Інтернет або базою даних за предметною тематикою НТІ безпосередньо в установі НТІ або навіть удома, біля власного комп'ютера).

Право розпорядження є юридично закріпленою можливістю власника самостійно вирішувати долю майна шляхом його відчуження іншим особам. Воно також включає можливість зміни стану майна та його призначення. Це право набуває особливого значення при здійсненні господарських або організаційних заходів щодо структурованих інформаційних масивів (фондів, баз або банків даних тощо)¹⁸¹. Наприклад, зміна стану такого майна при приватизації чи заміні власника виробництва, до якого належить масив ЗІР; продаж частини або й усієї БД, вилучення БД за однією предметною галуззю і передача (на певний час) іншому власнику; передача у вигляді внеску до господарського товариства тощо.

Щодо системи науково-технічної інформації та її ролі у підтриманні та розвитку новітніх технологій, які є результатом творчої діяльності українських вчених та винахідників, то це значною мірою залежить від загальної спрямованості розвитку нашої держави, від того, наскільки вона здатна оцінити інтелектуальний потенціал нації, створити сприятливі умови для впровадження кращих науково-технічних досягнень на внутрішньому та зовнішньому ринках. При цьому дуже важливим аспектом є правовий захист цих інновацій, адже в умовах жорсткої конкуренції, внаслідок їх незахищеності наша країна втрачає не тільки великі кошти, а й позиції рівноправного партнера.

У світовому співтоваристві все підпорядковується ринковим відносинам, до яких прагне приєднатися і наша країна. Тому так гостро постає питання збереження основного стратегічного для будь-якої країни товару — національного доробку з наукової, технічної і загалом інтелектуальної творчої діяльності.

У сучасній практиці реформування власності головна увага зосереджена на юридичному змісті власності¹⁸². З огляду на інформаційний ресурс найбільш вагомою є думка¹⁸³ щодо визначення самого поняття «інформація» і його використання у правознавстві.

Так, інформація у Законі України «Про інформацію» (ст.1) визначається як «документовані або публічно проголошені відомості про події і явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі». Серйозний сумнів викликають у автора¹⁸⁴ терміни «події» та «явища»: «в правовій літературі поняття «події» розуміється як один із видів юридичних фактів, з якими закон пов'язує виникнення, зміну або припинення правовідносин, що настають незалежно від волі людини (наприклад, повинь, землетрус, смерть тощо). Це поняття в правознавстві загальновизнане. У Законі «Про інформацію» цей термін вживається в іншому значенні, яке не збігається з загальновизнаним». Те саме стосується і поняття «явище». Безумовно, в законі потрібно дати визначення чи уточнення цих термінів, які були б обов'язковими для вживання у підзаконних актах, нормативній документації. До того ж при невизначенні або неналежному правовому тлумаченні цих термінів виникає неможливість застосування ст. 53 цього закону (абз. 2): «До інформаційних ресурсів України входить вся належна їй інформація, незалежно від змісту, форм, часу і місця створення»¹⁸⁵.

Ще більшої складності набувають питання права щодо НТІ (див. п.2.1.2). Справді, НТІ — це документовані або публічно оголошені відомості про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої і громадської діяльності (Закон України «Про науково-технічну інформацію»). Ці досягнення мають бути «зафіксовані у формі, яка забезпечує їх відтворення, використання і поширення»¹⁸⁶. Наприклад, звіти про НДДКР та їх повнотекстове розміщення у базі даних установи, яка зберігає такі відомості. Право власності на звіт за відповідною тематикою досліджень (навіть не на самі результати НДДКР, які не є у 99% випадків патентозахищеними) належить авторам НДДКР у особі наукового керівника розробки. Право користування і розпорядження передається установі, яка приймає цей звіт на зберігання. Право користування здійснюється установою через «аналітично-синтетичну обробку науково-технічної інформації» (ст.1, абз.8), а саме: «процес обробки інформації за методом аналізу і синтезу змісту документів з метою одержання необхідних відомостей, а також

шляхом їх класифікації, оцінки, зіставлення і узагальнення». Тобто установа-депозитарій створює уже власний інформаційний продукт і надає його в обіг, отримуючи від цього певні економічні та фінансові вигоди. Особливо це стає помітним, коли такі вторинні відомості використовуються у маркетинговій чи експертній діяльності. Власник документа (первинних відомостей) вже є відстороненим від цієї діяльності, і, таким чином, ці вторинні відомості становлять «об'єкт права інтелектуальної власності», а відносини щодо їх придбання, зберігання, переробки, використання і поширення регулюються чинним законодавством (ст.2, абз.4). Але, не визначивши чіткого розмежування між НТІ як документованими відомостями, що належать власнику — створювачеві результатів НДДКР, та НТІ як систематизованим зібранням «звітної науково-технічної документації» (ст.1, абз.4), що належать установі-депозитарію, неможливо здійснювати право розпорядження щодо таких «систематизованих зібрань» « документованої інформації». Тим більше ці невизначеності та невідповідності даються взнаки зараз, коли складаються умови щодо створення інфраструктур з просування вітчизняних розробок за кордон та замовлень із-за кордону на виконання наукоємних робіт для розміщення їх в Україні.

НТІ, по суті, не має захисту як літературний твір або науково-технічна продукція і водночас широко використовується при реалізації інноваційної політики, що ґрунтується на дії економічних законів ринку і науково-технічного прогресу.

Будь-яка змістовна інформація не тільки має своє матеріальне відтворення (у вигляді відомостей, даних, масиву тощо), а й надається через відповідну організаційну форму тому, що процес надання передбачає, як мінімум, наявність двох учасників. А в сучасному світі одним із таких учасників може бути просто комп'ютер.

Тому надзвичайно важливим є впорядкування на законодавчому рівні організаційно-суспільних відносин та велика увага щодо державних важелів перерозподілу власності, зокрема й у системі національних інформаційних ресурсів (СНІР).

Упродовж останніх десятиліть у працях багатьох науковців більш виразно подається структура категорії власності, зокрема розкриваються взаємозумовленість і відмінність власності

юридичної та власності економічної¹⁸⁷, що формує методологічну основу для подальшого дослідження різних напрямів розгортання економічного змісту власності в специфічних умовах ринкової трансформації суспільства.

Поглиблення знань про економічний зміст категорії власності має відбуватися в напрямі дослідження реальних форм її прояву в процесі виробничої господарської діяльності, у тому числі СНІР України.

Щодо ЗІР НТІ, то це змістовна інформація, яка створюється як поза межами власне інформаційної інфраструктури, так і є продуктом інтелектуальної праці людей, предметом діяльності яких є фахове виконання робіт із «збирання, аналітично-синтетичної обробки, фіксації, зберігання, пошуку та поширення НТІ» (Закон України «Про науково-технічну інформацію», ст.1, абз.3).

Таким чином, зміст категорії власності переводиться в площину: що привласнюється, хто і як привласнює, але не тільки з юридичного погляду, а і з урахуванням економічного змісту взаємопов'язаних факторів. Юридичні категорії об'єкта власності та суб'єкта власності переходять відповідно до категорій матеріально-речових і особистих, суб'єктивних факторів виробництва, а неодмінна юридична вимога — умови здійснення права власності — трансформується у категорію господарського механізму реалізації власності. Економічний зміст власності у такий спосіб переводить її до безпосередніх умов виробництва.

Як зазначалось (п.1.3), організаційні елементи інформаційної інфраструктури (ПФС), у межах якої формується змістовний інформаційний ресурс за результатами науково-технічної діяльності можуть виступати економічними суб'єктами як підприємницької і господарської діяльності, так і міжнародного процесу збагачення інформаційного ресурсу через обмін окремими відомостями за вітчизняним науково-технічним доробком у правовому полі нашої держави. Відповідно ці економічні суб'єкти підпадають під дію міжнародного права і вітчизняного законодавства в сфері формування та розвитку СНІР.

Саме тому підготовці будь-яких організаційних чи управлінських рішень з питань функціонування СНІР, регулювання інформаційних потоків, вирішення питань захисту та безпеки тощо має передувати певна програма організаційно-економічних та правових регуляторних чинників, побудована за прин-

ципом функціонального зв'язку з урахуванням впливу відповідних міжнародно-правових норм на світовому ринку інформаційних продуктів та послуг. Такий підхід мав би застосовуватись при прийнятті рішень щодо впливу зовнішніх змістовних інформаційних потоків на національну економіку не тільки урядом, міністерствами, відомствами, а й підприємствами (фірмами, товариствами тощо) при реалізації конкретних виробничих завдань, інвестиційних проектів, особливо з використанням іноземного капіталу (див. п. 3.3).

Усі ці питання пов'язані зі структурною побудовою ПФС, передусім з організацією структури НТІ як такої (не тільки системи центрів НТЕІ), що безпосередньо стосується процесів формування, розвитку, функціонування СНІР за національним науково-технічним доробком.

Механізм правового регулювання ЗІР НТІ має сприяти використанню повною мірою творчого потенціалу інформаційного ресурсу держави, регламентувати правові, економічні, організаційні відносини створювачів, власників та користувачів інформації в умовах ринку.

В інформаційному просторі зазвичай задіяні п'ять суб'єктів права:

- суб'єкт, що створює інформацію;
- постачальник інформації (до мережі, ІПС, масиву, фонду);
- «передавач» інформації (по мережі, ІПС, БД тощо);
- «приймач та «розподільник» інформації (частково ці функції нині здійснює інститут інформаційних посередників або провайдерів БД);
- споживач інформації (з мережі, ІПС, фонду тощо).

Саме між ними і розподілені права, обов'язки та відповідальність за все, що відбувається в мережі. Тому, коли спрацює (при наданні — передачі — отриманні змістовних даних) весь ланцюжок із згаданих суб'єктів, і всі ці суб'єкти можуть бути представниками різних країн, де діють різні правові норми та різні ступені відповідальності за різні правопорушення, стає очевидним складність питань права в інформаційній сфері.

Питання полягає в тому, як регулювати діяльність структур, які створюють інформацію, здійснюють доступ, розміщу-

ють інформацію тощо, а їх розв'язання визначатиме відповідні напрями розвитку СНІР.

Застосування базових законів інформаційної сфери «Про інформацію», «Про науково-технічну інформацію», у тому числі використання їхніх положень при формуванні підзаконних урядових актів, відомчих нормативних положень, включення основних положень у нормотворчість інших напрямів — економічну сферу, соціальну проблематику тощо, потребують суттєвого перегляду інформаційного законодавства України, включаючи зміни чинних документів з урахуванням історичних аспектів та накопиченого досвіду їх застосування. Зокрема, тісніша взаємодія з Європейським Союзом зумовлює необхідність врахування його директиви щодо побудови інформаційного суспільства. Це також стосується національних законодавств розвинутих країн, передусім США.

Найбільш активно потрібно використовувати положення базових законів стосовно галузей, які виробляють ЗІР: статистику, економіку, науки. Назріла також необхідність законодавчого вирішення питання щодо інформаційного ресурсу (в цілому), інформаційних продуктів та послуг як товару в аспекті їх надання через телекомунікаційні мережі. Ця остання проблема тісно пов'язана із питаннями власності на інформаційні ресурси. Тим більше, що нині спостерігається тенденція відходу від цього напряму та виникає прагнення використовувати такі юридичні поняття, як «володілець» (не власник, *рос.* — собственник), «розпорядник» або обмежитися лише авторським правом.

Виник ще один аспект представлення ЗІР — віднесення його до категорії нематеріальних активів, з чим тісно пов'язане поняття виключних прав юридичних осіб. У цьому ж, правовому, ряду стоять питання ціноутворення, витрат при створенні ШП, обміну ЗІР через Інтернет.

Однією з найголовніших є проблема ліцензування діяльності, пов'язаної зі створенням ЗІР та наданням, на його основі, ШП. До неї прилучається питання цілі використання інформації.

Згадані закони України встановили правові норми, які наголошують на бажаних відносинах в інформаційній сфері, а звідси їх декларативність та досить слабка дієвість у сучасних складних умовах суспільно-економічних реформ. Розробка доповнюючих нормативно-правових актів, спрямованих на регулювання

відносин суб'єктів суспільства у сфері виробництва та споживання (використання) інформаційних продуктів та послуг, здійснюється в напрямі інформатизації, що не враховує і, за своєю суттю, не може враховувати наслідки процесів інших суспільних сфер, які формують та використовують ЗІР. Особливо потрібно відзначити відсутність положень щодо правових механізмів підвищення ефективності використання накопиченого ЗІР у сучасних умовах, навіть у таких серйозних законопроектах, як проект Інформаційного кодексу України¹⁸⁸. Суттєвим сьогодні є й те, що розробка проектів нових законів, як-от Інформаційного кодексу, має супроводжуватись розробкою пов'язаних з ним змін та доповнень до Цивільного, Кримінального кодексів України та Кодексу України про адміністративні правопорушення.

Незважаючи на порівняно мале поширення системи Інтернет в Україні через низькі доходи основної маси населення, цей сегмент розвивається досить високими темпами (див. п.1.1). Але процес реалізації правових засобів регулювання відносин, що при цьому виникають, відбувається вкрай повільно, відсутні вторинні нормативні акти, які розвивали б положення законів України, зокрема про ліцензування нових видів послуг, що надаються у мережі; сертифікацію програмно-апаратних засобів, що використовуються для підприємницької діяльності у мережі. Нормативно-правове забезпечення українського сегменту Інтернет має ґрунтуватися на принципах, які включають стимулювання використання мережі, у тому числі при здійсненні державних закупівель товарів та послуг, пріоритет ринкової ініціативи в розвитку Інтернет, дотримання прав власності (інтелектуальної та майнової) на інформаційні продукти, які використовуються у мережі (див. п. 2.3.1).

Слід додати, що з розвитком ринкових відносин у інформаційній сфері виникає новий вид власності — інвестиційний, який пов'язаний з майновими правами створювача ШП (інформаційних продуктів і послуг).

Потребують також окремого уважного розгляду та опрацювання проблеми, що стосуються інформаційної частини майна підприємств та організацій, яке ґрунтується на державних інформаційних ресурсах, особливо у зв'язку з процесами приватизації та акціонування таких підприємств.

Складною проблемою залишається регулювання співвідношення інтересів, прав і обов'язків суб'єктів суспільних інформаційних відносин, пов'язаних із забезпеченням інформаційної безпеки, її важливої складової — захистом інформації та сфери обігу інформаційних ресурсів. Розвиток національної складової глобальної інформаційної мережі Інтернет потребує чіткого правового визначення вимог щодо інформаційної безпеки, захисту інформації та права на інформацію. Поширені серед певної частини науковців і спеціалістів погляди про те, що національний сегмент глобальної мережі, який об'єднує територіально розподілені комп'ютерні системи, має діяти лише за правилами, встановленими для всесвітньої мережі — є помилковими і можуть породити негативні наслідки. Корпоративні комп'ютерні системи призначені для обробки і поширення, в тому числі інформації обмеженого доступу, а також інформаційних ресурсів, які є інтелектуальною власністю. Система захисту від несанкціонованого доступу в таких мережах має відповідати правовому режиму інформації, що в них циркулюватиме. Окрім того, доцільно врахувати, що інформаційно-телекомунікаційні системи в Україні, в тому числі корпоративні й навіть спеціалізовані, створюються на базі засобів зв'язку та обробки інформації іноземного виробництва, здебільшого за архітектурою відкритих систем. У таких умовах розраховувати на запобігання можливого несанкціонованого доступу програмно-апаратними засобами є проблематичним. Тобто для захисту інформації, сфери її обігу та права на інформацію доцільно впровадити ефективні правові механізми та відповідні організаційні заходи. (Положення, що стосуються регуляторного права щодо СНІР України, зокрема процесів обміну **НТІ**).

Як зазначалось, всі основні положення про національну систему НТІ, її державного та підприємницького секторів, містяться в Законі України «Про науково-технічну інформацію», але, на жаль, вони не набули подальшого розвитку, що особливо помітно порівняно з ситуацією, яка склалася у Російській Федерації, у державній системі НТІ РФ.

З цього погляду одним із ключових завдань ДСНТІ є забезпечення інформаційної підтримки міжнародного науково-технічного співробітництва російських вчених та фахівців. Серед питань, пов'язаних з цим, ключовими, найважливішими є¹⁸⁸:

— ефективні механізми входження російських наукових колективів до міжнародних проектів і програм, що стосуються суверенітету країни;

— можливості вільного обміну інформацією поза будь-якими державними та відомчими бар'єрами;

— інформаційні супермагістралі та національна інформаційна політика;

— законодавче регулювання інформаційних процесів у зв'язку із зростанням соціальної та фахової залежності людини від можливості отримання інформації;

— організаційні структури та взаємозв'язок міжнародних організацій в інформаційній сфері.

В умовах розвитку в Росії федералізму, розбудови ринкових відносин і роздержавлення господарюючих суб'єктів, активного використання комп'ютерів та доступу до Інтернет найбільш важливим є зміцнення організаційної структури (інфраструктури) НТІ та нормативно-правове забезпечення сфери її діяльності. Можна стверджувати, що Положення про державну систему науково-технічної інформації РФ (затверджене постановою Уряду РФ від 24 липня 1997 року № 950) стало організаційно-правовим підґрунтям діяльності інфраструктури органів НТІ Російської Федерації.

Новим принциповим моментом у процесі відновлення ДСНТІ є записана у положенні відповідальність органів системи за організацію використання накопиченої (та накопичуваної) інформації. Ця функція визначена й у спеціальній програмі Міністерства промисловості, науки і технологій РФ «Створення, розвиток та організація ефективного використання державного інформаційного ресурсу».

Чільне місце в організаційній структурі НТІ РФ посідає ВІНІЛ (Всеросійський інститут наукової і технічної інформації), який з 1998 року було затверджено головною організацією відновлюваної ДСНТІ Росії. Без перебільшення можна стверджувати, що ДСНТІ відтворює — функціонально і структурно — процеси перерозподілу інформації, що становить основу державних процесів управління країною. У цьому плані робота керівного органу (Міністерство промисловості, науки і технологій) зосереджується на двох напрямках: збереження за Росією статусу найбільшого генератора інформаційних ресурсів та коорди-

нації робіт щодо відновлення та вдосконалення функціонування ДСНТІ РФ¹⁹⁰.

Істотною складовою системи НТІ РФ є об'єднання «Росінформресурс», до складу якого входять 69 центрів НТІ, ВІНІТІ та 45 міжгалузевих центрів НТІ. Ці центри є розпорядниками інформаційного ресурсу (ІР) держави відкритого характеру. Іншою складовою є система органів НТІ, головною серед яких функціонально є ВІМІ з 45 центрами, які є невід'ємною частиною установ, підприємств та організацій, яким вони підпорядковані (п.1.3).

Треба підкреслити, що на сьогодні у Росінформресурсі майже немає «чистих», спрофільованих тільки на НТІ організаційних структур. Як наслідок, у єдиному інформаційно-технологічному комплексі Росінформресурсу поряд з НТІ здійснюється збирання, обробка та поширення інших видів інформації, необхідної підприємствам та організаціям не тільки для науково-технічної діяльності, а й для їхньої економічної та юридичної практики. У цілому ж, поширюючи чи сприяючи обмінові інформації про результати науково-технічної діяльності, Росінформресурс став посередником між ринком та створювачами науково-технічної продукції. Тому з 1998 року розробляється та впроваджується загальноросійська система моніторингу нової науково-технічної продукції, що, безумовно, потребує тісного співробітництва з територіальними органами влади. Тільки їх підтримка на місцях може стати засадами ефективної діяльності державної системи НТІ РФ.

Відповідно до ситуації, що склалася, за завданням Державного комітету РФ по зв'язку та інформатизації була розроблена та затверджена (25 січня 1998 року рішенням Державної комісії з інформатизації при Держкомзв'язку Росії) Концепція управління діяльністю з формування, використання, ведення та захисту державних інформаційних ресурсів¹⁸¹.

У концепції пропонується визначення державних ІР як «створених за участю держави і за рахунок платників податків». До них віднесені такі види інформаційних ресурсів:

— створені за рахунок або з використанням коштів державного бюджету, бюджетів суб'єктів РФ, коштів органів місцевого самоврядування або коштів позабюджетних державних фондів;

— ресурси, які перебувають в оперативному управлінні державних і муніципальних установ, казенних та державних унітарних підприємств, а також некомерційних організацій, створених за участю держави;

— ресурси, що перебувають у господарському віданні акціонерних товариств з державним контрольним пакетом (див. п.1.3).

Усі зазначені види ІР мають бути охоплені відповідним нормативно-правовим забезпеченням, що має свої специфічні ознаки і створює предметну галузь чинного законодавства РФ. З погляду на розвиток НТІ як системи вимагають доповнень та змін закони РФ, що так чи інакше стосуються сфери НТІ, а саме: «Про інформацію, інформатизацію та захист інформації», «Про інформаційне забезпечення органів державної влади», «Про державний земельний кадастр», «Про внесення змін до федерального закону «Про обов'язковий примірник документів», «Про персональні дані», «Про державну статистику» та інші. У межах Кодексу РФ про адміністративні правопорушення вже внесені відповідні зміни щодо конкретного механізму застосування санкцій до органів та організацій за порушення правил формування та використання державних ІР, зокрема, визначення фактів порушення та відповідних штрафних санкцій за певні види порушень.

На макрорівні принципово важливою є виважена інтеграційна політика України. Найбільш актуальними є формування режиму вільного руху товарів, а також ефективна міжнародна інвестиційна взаємодія з країнами СНД.

Зрозуміло, що для органічного входження до економічної системи СНД, Європи необхідні цілеспрямовані правові та інституційні заходи.

Сьогодні існують різні варіанти «інтеграційної поведінки» України у межах СНД, де формуються як нові взаємовідносини на двосторонній основі, так і секторальні (галузеві), субрегіональні та наднаціональні інтеграційні структури.

Так, враховуючи світові тенденції до співробітництва та спільного використання науково-технічної інформації, уряди 10 країн СНД — Вірменія, Білорусь, Грузія, Казахстан, Киргизстан, Молдова, РФ, Таджикистан, Узбекистан та Україна — в Мінську 26 червня 1992 року уклали Угоду про міждержавний обмін науково-технічною інформацією (МОНТІ)¹⁹².

Тоді ж були визначені основні напрями МОНТІ: формування ІР спільного користування; спільне формування та використання ІР, що відбиває світовий потік НТІ; здійснення спільних науково-технічних програм, проектів міждержавного співробітництва в галузі НТІ, що включали підготовку та перепідготовку кадрів; інформаційна підтримка міждержавного науково-технічного співробітництва. При цьому міждержавний обмін НТІ мав здійснюватись інформаційними центрами держав — учасниць угоди (колишні центри науково-технічної та економічної інформації республік СРСР) на концептуальних та методологічних засадах, що приймалися спільно, які забезпечували б правову, технічну та технологічну сумісність такого обміну.

У листопаді 1995 року уряди держав — учасниць СНД підписали Угоду про створення спільного науково-технологічного простору. Розуміння такого простору містить сукупність середовища забезпечення функціонування і розвитку науки і технологій, яке характеризує єдина державна науково-технічна політика. Ця політика спирається на адекватну нормативно-правову базу і включає перелік національних пріоритетів, системи управління науково-технологічним розвитком, фінансування, підготовку та атестацію наукових та інженерних кадрів, науково-технічну інформацію, стандартизацію, метрологію, сертифікацію, охорону прав на результати науково-технічної діяльності.

Для реалізації цієї угоди створений Міждержавний комітет з науково-технічного розвитку (МК НТР), що діє при Міждержавному економічному комітеті Економічного Союзу (МЕК). МК НТР діє в тісному співробітництві з іншими міждержавними та міжурядовими органами СНД, а також Міжнародною асоціацією академії наук (МАН).

До плану першочергових заходів зі створення спільного науково-технологічного простору держав — учасниць СНД, затвердженого колегією МЕК СНД, були включені планові роботи МКР НТІ. Згідно з цим планом у 1996 році був підготовлений проект міждержавної Угоди про вільний доступ та порядок обміну відкритою науково-технічною інформацією. За цією угодою держави-учасниці мають забезпечувати вільний доступ до відкритої НТІ та даних, що не мають комерційного характеру, та домагатимуться скасування в межах СНД митних обмежень при передачі наукової літератури та НТІ. Відповідно до цієї

угоди органи державного управління здійснюють заходи з прийняття відповідних національних нормативно-правових актів.

З 1998 року по теперішній час МКР НТІ планував узяти участь у розробці документів, що готувалися виконавчим секретаріатом СНД у межах реалізації концепції реалізації єдиного інформаційного простору (Україна зголосилася брати участь у його створенні, але з деякими застереженнями, які не дали змоги їй підписати документ у цілому), зокрема¹⁹³:

- створення системи міжбібліотечного абонементу держав — учасниць СНД (діє з 1998 року);

- підготовка модельного законодавчого акта з НТІ;

- координація формування та використання інформаційних ресурсів держав — учасниць СНД за узгодженими сферами діяльності;

- створення Міждержавного реєстру національних інформаційних ресурсів держав — учасниць СНД за узгодженими сферами діяльності;

- пропозицій про вибір пріоритетів при обміні ІР у межах СНД;

- концепції забезпечення інформаційної безпеки СНД;

- співробітництва в галузі забезпечення інформаційної безпеки.

Розробка та прийняття зазначених документів дали б змогу суттєво просунутись у галузі створення дієвої нормативно-правової бази щодо забезпечення, насамперед організаційного забезпечення, міждержавного інформаційного обміну з урахуванням вимог інформаційної безпеки як складової національної безпеки країн — учасниць Співдружності.

На жаль, незважаючи на певні досягнення держав СНД у формуванні спільного інформаційного простору, аналіз результатів роботи свідчить, що вирішення цього завдання наштовхнулося на значні перешкоди як організаційного, так і економічного характеру, що серйозно стало перешкодою на шляху реалізації угоди. За дев'ять років свого існування у МКРНТІ тільки РФ, Республіка Білорусь та частково Україна надали свої внески на формування Фонду розвитку міждержавного обміну НТІ, результатом чого стало невиконання запланованих програм та проектів, у тому числі спільних науково-технічних програм. МКРНТІ з 2000 року функціонує під егідою Виконав-

чого секретаріату МЕК СНД як напрямок робіт, а не як окрема виконавча структура. Але, безумовно, подальший розвиток системи міждержавного обміну НТІ в організаційно впорядкованій структурі дав би змогу зняти багато суперечностей та вирішити багато питань з передачі НТІ та пов'язаних з цим проблем власності на науково-технічну продукцію. Взаємодія ж України з країнами СНД у науково-технічній сфері в даний час регламентується дво- та багатосторонніми угодами.

Отже, у процесі суспільно-економічної трансформації суспільства державна інформаційна політика є невід'ємною складовою соціально-економічної політики і в цьому аспекті спрямована на реалізацію стратегічних та тактичних цілей у сфері виробництва інформаційних продуктів та послуг за результатами наукової і технічної діяльності в Україні.

Законодавче визначення режиму змістовного інформаційного ресурсу сприятиме ефективності його використання в умовах реструктуризації власності та значною мірою розширенню інвестиційних можливостей держави, а значить перспектив економічного зростання і розвитку.

Складність економічного становища змушує організації та підприємства передавати ШП покупцям, у тому числі іноземним, нерідко без обґрунтованого економічного опрацювання. З іншого боку, те, що купується за кордоном, використовується не досить ефективно та без урахування загальнодержавних інтересів.

Негативні чинники, передусім правового характеру, можна згрупувати в такий спосіб:

- відсутність правових механізмів включення до господарського обігу та неналежна координація щодо використання інформаційних ресурсів веде до економічних втрат, посилення потенційних конкурентів;

- відсутність державної системи захисту та охорони прав власності на НТІ, відомча неузгодженість, брак уніфікованих заходів щодо забезпечення конфіденційності інформації, практично неорганізований контроль за експортом та імпортом наукоємних технологій призводять до втрат не тільки інформаційного характеру, наслідком є суто економічні та частково політичні втрати;

— відставання вітчизняних інформаційних технологій, не^врегульованість нормативних положень примушує масового споживача йти у напрямі закупівлі незахищеної імпоротної техніки, що сприяє поширенню несанкціонованого доступу до інформаційних ресурсів і підвищує залежність вітчизняних споживачів від виробників телекомунікаційної техніки і технологій.

До цього необхідно додати, що Закон України «Про обмеження монополізму та недопущення недобросовісної конкуренції у підприємницькій діяльності» на відносини, які виникають з прав на інформаційні об'єкти, не поширюється (докладніше див. у п.2.3.2).

При цьому слід підкреслити особливо про те, що використання змістовного інформаційного ресурсу за науково-технічним доробком, передусім із закритої тематики, гальмується недостатньо розвинутою вітчизняною нормативно-правовою базою, а в деяких випадках і діючими нормативними і керівними документами колишнього СРСР.

Слід зауважити, що в колишньому СРСР була створена логічно завершена система захисту державних секретів, в основу якої була покладена загальнодержавна форма власності на засоби виробництва і централізована система державного управління. Система захисту державної таємниці розглядалася як сукупність пов'язаних сил, засобів і спеціальних заходів, спрямованих на оптимальне обмеження сфери обігу державних секретів і запобігання їх витоку. З системного погляду її можна було б визначити як замкнуту регульовану систему, рамки якої обмежують допустимість використання секретної інформації в процесі наукової, виробничої, адміністративно-господарської або іншої службової діяльності підприємств, установ, організацій. При цьому враховувалося те, що секретна інформація або виникає як результат інтелектуальної діяльності виконавців робіт (документів), фіксується в свідомості осіб, які допущені для ознайомлення, або відображається на матеріальних носіях будь-якого роду чи виду.

У цьому контексті під витоком державних секретів слід розуміти неправомірний вихід державних секретів за межі встановленої для них сфери обігу, в результаті чого вони стають відомі стороннім особам.

За тих часів у СРСР каркасом у системі «наука — виробництво» були галузеві НДІ і КБ, академічні інститути, університе-

ти, окремі вузівські лабораторії, науково-виробничі об'єднання, вчені й інженери яких, використовуючи результати фундаментальних досліджень, створювали і засекречували нові знання в галузі математики, фізики, хімії, механіки, біології, наук про Землю, впроваджували їх у новітні системи озброєнь, авіаційну та космічну техніку, приладобудування, суднобудування тощо.

Розробники системи захисту державної таємниці в СРСР використовували для її створення вагоме науково-теоретичне підґрунття, положення теорії управління, зокрема, враховувався фундаментальний принцип кібернетики, відомий як принцип необхідного різноманіття У. Росса Ешбі, який, як відомо, коротко формулюється так: «Різнорманіття керуючої системи має бути не менше різноманіття об'єкта управління». Тобто з боку керуючого органу має існувати можливість використання визначених керуючих впливів та вибір необхідного впливу залежно від стану об'єкта управління¹⁹⁴.

З цього ж принципу випливає й те, що з ускладненням об'єкта управління складність керуючої системи має збільшуватися. Саме цей процес ми спостерігаємо сьогодні. За умов появи підприємств, установ і організацій різних форм власності, різноманіття організаційних форм суб'єктів господарювання, появи спільних підприємств, ускладнюються завдання щодо захисту національних інформаційних ресурсів у цілому і, зокрема, змістовного інформаційного ресурсу за науково-технічним доробком.

Водночас сучасні потреби вітчизняної науки і промисловості, глобалізація економічних зв'язків українських підприємств, перехід людства до нового технологічного укладу загострюють актуальність проблеми обґрунтованого введення в обіг накопиченої інформації подвійного використання, відкритості інформації про наукові дослідження та використання їх результатів у міжнародних науково-технічних проектах.

Характерно, що створення в Україні ще за радянських часів науково-технологічних комплексів у системі Академії наук, які відіграли винятково важливу роль у ефективному впровадженні досягнень науки у виробництво в умовах соціалістичної економіки, для яких характерна відсутність яскраво виражених меж між фундаментальною наукою та науковою технологією, сьо-

годні стало світовою тенденцією — відбувається переміщення наукових дослідницьких центрів до структур транснаціональних фірм, підпорядковане розв'язанню проблем комерціалізації «ноу-хау» до рівня прикладних технологій, спрямоване на їх продаж і швидке впровадження.

За новими матеріалами й технологіями стоїть добре організована система наукових досліджень, у світі виникла принципово нова ситуація: лідера практично неможливо наздогнати. Як свідчить досвід, секретною, наприклад у галузі неорганічної хімії, є 50 — 80 % інформації, що накопичується фундаментальною наукою. У прикладній науці з вивчення процесів у конкретних виробництвах частка нової секретної інформації становить 90 — 95 %. На ранніх стадіях наукового пошуку необхідність засекречування робіт визначається не лише сферою військового застосування, а й можливістю використувати отримані результати для розв'язання багатьох цивільних проблем.

Науково-технічна революція висунула на авансцену технолога, оскільки нова техніка сьогодні — це насамперед принципово нові матеріали і технології. Саме технологія акцентує сьогодні увагу світових виробників на проблематиці «ноу-хау» (секретів виробництва), які мають бути захищені від несанкціонованого використання третіми особами. Вона має справжню або потенційну вартість саме тому, що невідома третім особам.

Поняття «комерційна таємниця» істотно ширше, ніж «ноу-хау», оскільки її складають навіть списки клієнтів, первинні бухгалтерські документи і багато інших відомостей про організаційну й фінансову діяльність фірми. Ширшою за комерційну є державна таємниця. Вона може охоплювати відомості, що не мають ринкової вартості, або ті, які ніколи не виходять на будь-які комерційні ринки. Частина комерційної таємниці може належати до державної таємниці, що найбільш яскраво виявляється при торгівлі наукоємними озброєннями і військовою технікою.

Тенденція зростання ролі секретів виробництва в охороні технологій пов'язана з великою вартістю трансакційних витрат у процесі здійснення права на охорону об'єкта інтелектуальної власності та, більш того, при комерціалізації науково-технічних досягнень. Справді, тільки оформлення відповідних юридичних документів потребує залучення патентних повірених, ауди-

торів, незалежних оцінників, що є тривалим та дорогим процесом, як і доведення факту порушення патенту, якщо це мало місце, пов'язане з великими витратами на послуги патентних повірених, експертів та адвокатів, тобто з великими трансакційними витратами.

Фактично патентна охорона технологій стає доступною лише великим фірмам, причому надійність охорони не є забезпеченою і в цьому разі.

Збереження технології у секреті коштує значно дешевше. Більш того, надійність патентної охорони весь час знижується, тоді як надійність охорони секретів виробництва скоріш зростає, ніж падає. Витрати специфікації та охорони виключних прав зростають швидше, ніж при охороні тих самих технологій у режимі комерційної таємниці (секретів виробництва). Зовсім навпаки відбувається все при використанні тих же інституцій для охорони кінцевих продуктів. Встановити факт порушення патенту в цьому разі порівняно легко, а засекретити конструкцію майже неможливо. Тому патентна охорона дедалі більше рухається у напрямі охорони кінцевих виробів, тоді як для охорони технологій у її інформаційному аспекті дедалі більше використовується інституція комерційної таємниці.

Як свідчить світовий досвід, крім низки соціально-економічних заходів, для виведення країни з кризи, пожвавлення інноваційної діяльності реального сектору економіки потрібно і вирішення ряду правових питань у сфері інформаційних відносин, оскільки для стикування інтересів науки та виробництва дуже важливим є правове забезпечення інформаційної діяльності з урахуванням сучасних реалій.

Трансформація економічних відносин в Україні висунула на перший план проблему становлення системи відносин виробників інтелектуального продукту, захист їх прав і стимулювання інтелектуальної праці в ринкових умовах господарювання, оскільки науково-технічний потенціал — це насамперед висококваліфіковані наукові та інженерно-технічні кадри, які володіють відповідною мотивацією до ефективної інтелектуальної творчої праці.

Ця проблема набуває стратегічного значення і стає основою розвитку економіки, оскільки впровадження наукоємних технологій потребує, з одного боку, вузької спеціалізації фахівців, з

іншого — замикання ланцюжка «маркетинг — дослідні розробки — інвестиції — виробництво — збут» у рамках єдиного комплексу.

На законодавчому рівні потребують уточнення і конкретизації з урахуванням нових умов цілі, завдання та організаційні основи захисту інформації.

Нині спостерігаються такі дві основні тенденції щодо формування правового поля використання інформаційного ресурсу держави, як регулятивна та захисна. Регулятивна спрямована на визначення етапів виникнення, збирання, обробки, збереження та надання інформації і обумовлюється системою угод або домовленостей між власником першоджерел та розпорядником фонду даних чи певного типу відомостей. Захисна забезпечує порядок використання змістовних даних та визначає порядок доступу до організованих певним чином масивів інформації за допомогою відповідного інструментарію (у тому числі технічних, засобів).

Змістовний інформаційний ресурс, що вводиться до господарського обігу як стратегічний ресурс суспільства, може бути об'єктом власності різних суб'єктів господарювання та розглядатися як продукт переробки в різних інформаційних системах з правовим режимом обробки, яка встановлюється власником засобів обробки відповідно до визначеного чинним законодавством правового режиму його конкретного виду.

Тут є дієвими умови власника першоджерел та власника інформаційної системи як способу обробки та збереження змістовних даних першоджерела. Нова інформація як продукт обробки, що виникає згідно з конкретним технологічним циклом, який включає засоби обробки та персонал, є власністю господаря цих засобів або, за системою угод, власністю замовника опрацьованої інформації чи, за порядком інформаційного забезпечення, власністю користувача інформаційної системи. При цьому умови, за якими була здійснена передача першоджерела до інформаційної системи, є переважними, а тому права власника мають ураховуватися передусім при оплаті (чи в умовах передачі) нової, опрацьованої замовником.

Таким чином, щоб бути або стати компонентом змістовного інформаційного ресурсу, який використовується суспільством, інформація повинна мати визначений правовий режим на всіх

етапах свого виникнення, обігу, поширення. Це має бути зареєстровано та піддано для подальшого обліку відповідно до правових норм, виконання яких має контролюватися державою.

Зауважимо, що державою протягом останніх років вжито низка заходів щодо вдосконалення правового регулювання в інформаційній сфері, захисту її національних інтересів, водночас для розбудови інформаційного ринку, насамперед потрібне вдосконалення законодавчих актів України, які стосуються науково-технічної сфери, їх слід доповнити, зокрема, положеннями про формування та використання державних ресурсів НТІ, особливо незахищеної патентами інформації, з урахуванням глобалізації інформаційних мереж і електронних баз даних, інноваційної діяльності та захисту інтелектуальної власності на наукові, науково-технічні та технологічні розробки і науково-технічну продукцію¹⁹⁵.

До того ж найбільшим попитом як на внутрішньому, так і світовому ринках користується ЗІР за науково-технічним доробком оборонного та подвійного призначення. Кожна держава для такої інформації встановлює певні обмеження доступу і охорони (режими секретності і конфіденційності), які відповідають правовому режиму кожного виду інформації. Стосовно державної таємниці та іншої інформації з обмеженим доступом, що є власністю держави, — це право держави встановлювати порядок її виготовлення та використання. Щодо конфіденційної інформації, яка є приватною власністю, встановлення обмежень доступу та порядку використання — це справа власника цієї інформації, котрий вирішує ці питання в межах чинного законодавства.

Окремим питанням, що виходить за рамки цієї праці, є оцінка вартості змістовного інформаційного ресурсу, яка прямо пов'язана з визначенням вартості НДДКР. Система контролю використання коштів на наукову діяльність, яка заснована на формальній оцінці додержання нормативів трудовитрат і яка досить ефективно працювала в попередніх економічних умовах, за ринкових умов, де на перший план висувається цінність для науки і практики заявлених для розробки матеріалів, стає анахронізмом. Цінність може визначатися за двома напрямками: новизна дослідження і прогнозована якість результатів¹⁹⁶.

Визначена чинним законодавством необхідність використання інформаційних ресурсів України на основі рівноправного міжнародного співробітництва¹⁹⁷ стосовно сфери, пов'язаної з інформацією з обмеженим доступом, що не становить державної таємниці, та об'єктів промислової власності залишається поза межами правового регулювання.

Таким чином, важливим чинником підвищення ефективності використання змістовного інформаційного ресурсу за науково-технічним доробком є законодавче визначення правового режиму кожного виду інформації як основи для розробки і впровадження нормативно-правових і організаційних механізмів забезпечення права власності на інформаційні ресурси, прав суб'єктів України на одержання ЗІР на безоплатній і комерційній основі, використання їх для економічного і соціального розвитку країни та рівноправності в процесі міжнародного інформаційного обміну.

Для вирішення цього завдання, на думку автора, необхідно прийняти Закон України «Про державне регулювання діяльності у сфері трансферу технологій», який визначив би правові, економічні, організаційні та фінансові засади державного регулювання діяльності у сфері трансферу технологій з метою забезпечення ефективного використання науково-технічного та інтелектуального потенціалу України, підвищення технологічності виробництва вітчизняної продукції, охорони майнових прав на вітчизняні об'єкти технологій на території держав, де планується або здійснюється їх використання, розширення міжнародного науково-технічного співробітництва у цій сфері. Прийняття такого закону поряд з чинними Законами України «Про наукову і науково-технічну діяльність», «Про наукову і науково-технічну експертизу», «Про науково-технічну інформацію», «Про інноваційну діяльність», «Про власність», «Про охорону прав на винаходи і корисні моделі», «Про охорону прав на промислові зразки», «Про охорону прав на топографії інтегральних мікросхем», «Про авторське право і суміжні права», «Про зовнішньоекономічну діяльність», іншими нормативно-правовими актами було б суттєвим кроком щодо вдосконалення вітчизняного законодавства про державне регулювання діяльності у сфері трансферу технологій.

2.3. ІНФОРМАЦІЙНИЙ ОБІГ ТА ЗАХИСТ ІНФОРМАЦІЇ ЗА РЕЗУЛЬТАТАМИ НАУКОВО-ТЕХНІЧНОЇ ДІЯЛЬНОСТІ У ВІДКРИТОМУ ДЕМОКРАТИЧНОМУ СУСПІЛЬСТВІ

2.3.1. Специфіка використання національного інформаційного ресурсу у відкритому демократичному суспільстві

Сучасну світову тенденцію соціально-економічного розвитку і науково-технічного прогресу визначає рівень інтелектуалізації основних сфер виробництва і послуг. За оцінками експертів, нові знання, що втілюються в технологіях, обладнанні, освіті, підготовці кадрів, організації виробництва, в розвинутих країнах вже нині дають зростання економіки на 80 — 95%. Тому не є випадковим загострення боротьби за володіння інтелектуальними інформаційними ресурсами, за носіїв інтелекту і знань, за відкритість науково-технічної інформації, особливо подвійного та оборонного призначення.

Президент України Л.Д. Кучма у виступі на засіданні Державної комісії з питань стратегії економічного та соціального розвитку визначив завдання щодо розробки «Стратегії економічного і соціального розвитку України на 2002 — 2011 роки», спрямованої на забезпечення якісних зрушень в економіці. Як зазначав Президент України, «успіх може прийти лише за умови: якщо ми забезпечимо посилення регулюючої функції держави; якщо наявні матеріальні, людські та фінансові ресурси не будуть розпорошуватися; якщо ми переглянемо всі діючі програми і зможемо через механізми державного прогнозування забезпечити концентрацію існуючих ресурсів на реалізацію ключових завдань української економіки, утвердженні її конкурентних переваг, зміцненні та розвитку передусім наукоємних галузей виробництва, на забезпеченні науково-технічного прогресу»¹⁹⁸.

Виконання завдань, визначених Президентом України, залежатиме не лише від суто економічних чинників. Одним з таких факторів є інформаційна складова економічного і соціального розвитку, забезпечення важливих сфер життєдіяльності суспільства і держави.

Професор А. Гальчинський у публікації «Демократію — для всіх» на основі аналізу процесів утвердження сучасної європейської демократії, теоретичних засад її розвитку доводить, що розвиток демократичної системи можливий лише на еволюційній основі, що поглиблення демократії безпосередньо пов'язане з економічним розвитком, зростанням багатства нації та добробуту людей, упровадженням цивілізованого парламентаризму та підвищення дієздатності держави як «суб'єкта демократизації»¹⁹⁹. Критерій демократичності у фундаментальному дослідженні колективу авторів «Глобалізація і безпека розвитку» віднесено до комплексу критеріїв оцінки сучасного світового та економічного порядку. У цій праці відмічено, що процеси прискореної демократизації більш характерні для суспільств так званого перехідного стану: «Щонайперше суспільства таких держав повинні самоусвідомити фундаментальну сутність феномену демократії та її роль у соціально-економічних процесах. ...Феномен демократії є соціально-економічним функціоналом, а не тільки деякою політичною чи ідеологічною категорією. Головним своїм важелем вона спрямована на якнайшвидше досягнення достовірних (істинних) інформаційних знань у всіх сферах, пов'язаних із соціально-економічним життям, передусім у сфері державного управління»²⁰⁰.

І ще один аспект, що має важливе політичне звучання, пов'язаний із змістом нового Цивільного кодексу України. Законодавець, маючи намір створити кодекс приватного життя держави, сформулював його норми, допускаючи протиставлення держави і громадянського суспільства. Держава розглядається не як необхідний продукт громадянського суспільства, а як суб'єкт, що протистоїть суспільству у вигляді владної бюрократичної структури, що лише громадянське суспільство має захищати приватні інтереси від бюрократичного втручання держави. При цьому слід зауважити, що Конституцією Україна проголошена демократичною, правовою державою, тому неприпустимо у будь-якому акті законодавства уявляти державу як антигромадянську, антисуспільну надбудову, ігноруючи її позитивний соціальний потенціал. Держава має відігравати дедалі активнішу роль у житті як суспільства, так і окремої особи, в тому числі в правовому регулюванні суспільних економічних,

інформаційних тощо відносин. Особливо важливого значення набуває регулююча роль держави для впорядкування відносин, пов'язаних з використанням національних інформаційних ресурсів.

У світовій політичній думці логічно поєднуються поняття «демократизація, децентралізація і розвиток». Базовими є такі форми децентралізації: політичні, просторові, ринкові та адміністративні. З цього виводяться типи управлінської децентралізації — зниження концентрації влади, передача більшого кола повноважень місцевим органам влади та делегування обов'язків згори донизу. Політична форма передбачає максимальну передачу розробки і прийняття рішень урядовим інститутам нижчого рівня, громадам чи їх обраним представникам. Просторова децентралізація стосується регіонального і місцевого планування з урахуванням географічних показників і використовується при визначенні та формулюванні цільових програм регіональних і локальних полюсів розвитку. Ринкова децентралізація застосовується для аналізу і запровадження в управлінську практику планів, стратегій і дій з оптимізації умов виробництва на засадах ринкових механізмів. Така форма демократизації управління визнана вирішальною²⁰¹. Адміністративна децентралізація включає розподіл функцій між центральними, регіональними і місцевими органами влади на чіткій політико-правовій базі. Функціональне претендування вищих ешелонів влади на верховенство обов'язково виключається законом.

Світовий, зокрема азіатський, досвід підтверджує, що на певному етапі суспільного розвитку необхідність інвестицій і поліпшення фінансового стану наштовхується на централізацію влади. Постає об'єктивна потреба в переході до диверсифікованої системи державного управління. Надмірна централізація управління, зокрема у сфері інформаційної інфраструктури, виливається у нездатність вчасно і якісно реагувати на суспільні потреби у цілому. Економічне зростання в цих умовах залежить від здатності влади кооперувати з бізнесом. Відмова від командних методів у відносинах з бізнесом потрібна завжди, навіть коли такі методи видаються тимчасовими.

Успішне функціонування ринку у сфері інформаційних ресурсів залежить також і від того, що нинішня епоха інформаційної економіки, побудована на демократичних засадах, суттєво

відрізняється від індустріальної і навіть «комп'ютерної» епохи. Остання мала на меті автоматизацію «паперової» роботи та підвищення ефективності бізнесу за рахунок повсюдного впровадження комп'ютерної техніки і була, за своєю сутністю, останнім досягненням індустріальної епохи. У результаті здійснився реінжиніринг (реорганізація) бізнес-процесів, що дало змогу установам, підприємствам та організаціям відповідно до принципів функціонування та розвитку епохи індустріалізації певним чином оптимізувати свою роботу та продовжити розвиток у нових демократичних умовах.

Суть нової інтелектуально-інформаційної глобалізації полягає в перетворенні інформаційних технологій на головний інструмент створення вартості продукції нового типу «high-hume prodacts» на відміну від «high-tech» продукції. Провідні лідери глобалізації перенесуть традиційне виробництво у відсталі країни, а в себе розвиватимуть високоінтелектуальне виробництво і виробництво нових принципів і технологій управління. В умовах глобалізації експорт капіталів буде замінено експортом технологій²⁰².

Приматом та імперативом для нових незалежних країн є високоефективний державний менеджмент, здатний розробляти і втілювати в життя економічну стратегію і національну стратегію розвитку, орієнтовану на врахування вимог і законів глобалізації і глобальної інтеграції, здатну вирішувати довгострокові завдання розвитку на десятиліття вперед, спроможну забезпечувати необхідні масштаби і високу якість внутрішніх соціально-економічних трансформацій²⁰³.

Така перебудова, як засвідчує практика, відбувається в результаті та завдяки широкому використанню інформації.

Найпершим питанням стосовно інформації в будь-якому демократичному суспільстві є доступ громадськості до інформації та власність на неї. З цим пов'язане питання про передбачуваність ролі уряду щодо надання інформації, тобто чи буде уряд активним поширювачем та розподільником інформації, чи лише пасивним респондентом.

Юридичною властивістю змістовної інформації при цьому є здатність виступати як об'єкт, що передається від одного суб'єкта взаємовідносин до другого. Ця здатність і потребує відпо-

відного юридичного закріплення факту належності об'єкта суб'єктам — учасникам ділових (або інших) обігів.

Одним із суттєвих попередніх висновків є те, що науково-технічна інформація, по суті, не має захисту як літературний твір або науково-технічна продукція. Водночас вона широко використовується при реалізації сучасної інноваційної політики, яка ґрунтується на дії економічних законів ринку і науково-технічного прогресу (див. п. 2.1).

Тому, не визначивши чіткого розмежування між НТІ як документованими відомостями, що належать власнику — створювачеві результатів дослідження (НДДКР), та НТІ як систематизованим зібранням звітної науково-технічної документації, що належить установі-депозитарію, неможливо здійснювати право розпорядження щодо таких систематизованих зібрань документованої інформації без попередньо обумовлених договором умов використання та надання в користування цих даних.

Закріплення абсолютних прав власності суб'єктів на інформацію обмеженого доступу передбачає впровадження державою певних правових механізмів забезпечення цих прав. Наприклад, визначальним критерієм щодо державної таємниці є належність державі засекречуваних відомостей. Тобто держава правовими нормами встановлює режим доступу та порядок використання такої інформації. Стосовно інших передбачених законодавством таємниць та конфіденційної інформації чинне законодавство²⁰⁴ надає право власникові встановлювати обмеження доступу та порядок використання такої інформації. Значно складнішим є питання щодо забезпечення права власності на відкрити інформацію саме з погляду на її загальну доступність.

Слід зауважити, що вже неодноразово на практиці виникала ситуація, за якої продукт, наданий на ринок (наприклад, база даних), копіювався і незаконно поширювався. Але суб'єкт, що привласнив згаданий продукт, не витратив коштів на його первісне створення, тому ціна такого повторного поширюваного продукту відчутно знижується, а виробник зазнає значних втрат. Порушення ж прав власності на документовану інформацію при цьому не відбувається, тому що масив документів у виробника не відчужувався. Такі дії мають бути кваліфіковані як недобросовісна конкуренція і відповідно припинені²⁰⁵.

Рішенням могло б бути закріплення виключних прав на інформаційні ресурси з погляду на їх зміст або вдосконалення чинного законодавства про охорону «зібрань документованої інформації» та баз даних як їх машиночитного відтворення, результатом чого об'єктом захисту стане не тільки форма зібрання, а і його зміст. Для цього доцільно використати як правове підґрунтя інститут промислової власності, розроблений для охорони нематеріальних об'єктів, з реєстраційним порядком набуття права. Для захисту інформаційних ресурсів він має ту перевагу, що захист отримують лише безпосередньо зацікавлені в ньому суб'єкти²⁰⁶.

Концептуально НТІ може бути розглянутою як окрема галузь політики та політичного аналізу з огляду на її вагомість у соціальному, політичному, економічному та військовому аспектах. Має бути визначена роль інформації, зокрема НТІ, у процесі винахідництва в цілому й у процесі передачі технологій зокрема. Особливий наголос має бути зроблено на доступі до інформації за допомогою належної технології.

За досвідом США, захист НТІ включає чотири основних аспекти²⁰⁷. Перший визначає, що підлягає безпеці, хто може обмежувати доступ до НТІ (особливо, що надходить від владних структур) і на підставі яких санкцій.

Другий — визначення термінів: коли передавати НТІ, що є в державних депозитаріях та належить до державних структур, до приватного сектору. Звичайно, ті, хто не входить до уряду, бажають зменшити часові обмеження для того, щоб СІНА залишались конкурентоспроможними на академічному та комерційному ринках. Конверсія НТІ, яка створена у військовому відомстві, зазвичай ускладнена. Було прийняте рішення розділити технології таким чином, щоб виділити справді вирішальні військові технології. З одного боку, уряд СІНА може забезпечити охорону певних ініціюючих технологій у галузях, в яких США мають незаперечну технологічну перевагу, з іншого — досягається більша відкритість у галузях, в яких країна не є єдиним лідером.

Третій — врахування комерційної цінності секретної інформації. Коли на часі є концепція прогресу в необмеженому потоці певної інформації, мають бути розглянуті інші мотиви, поза комерційною користю.

Четвертим аспектом є порівняння вартості та ризику. Класичним критерієм при визначенні безпеки має бути положення: вартість запобіжних заходів не більша, ніж ризик від отримання вільного доступу до інформації. Зрозуміло, що суттєвим питанням тут є питання балансу між охороною інформації та її доступністю.

Усі ці питання, у тому числі передача і захист інформації, пов'язані з науковими дослідженнями та промисловою інновацією. Багато промислових галузей України вже тривалий час мають тісний та продуктивний зв'язок з науковою базою, що, зрештою, доводить практика таких сучасних інституцій, як технопарки, наукогради тощо.

Водночас уряди технологічно передових країн продовжують удосконалювати систему заходів, що забезпечують перевагу своїм фірмам у випадку передачі ними технологій²⁰⁸.

Тому сьогодні правові документи чи нормативні акти, пов'язані з передачею або з наданням змістовно вагомої інформації, набувають таких рис, як:

- надання прав державі визначити корисність запропонованої для введення технології;
- держава бере участь у вирішенні всіх питань, що стосуються передавання такої інформації;
- встановлюється порядок обов'язкової реєстрації угод, у тому числі міжнародних, і одержання схвалення компетентних органів, які перевіряють угоди з економічного, технологічного, правового, соціального та політичного поглядів з метою оцінки дійсної корисності для розвитку країни.

У переважній більшості країн (СІНА, Велика Британія, Німеччина, Японія, Індія, Фінляндія, Мексика, Ямайка тощо) нормативні акти регламентують зміст договорів через визначення: умов, узгоджених у договорі в обов'язковому порядку; умов і застережень, наявність яких у договорі може стати підставою для відхилення реєстрації.

Органи державного регулювання не тільки контролюють ліцензійні угоди, а й вимагають, за необхідності, внесення змін до угод або навіть до законодавчих актів.

Упродовж останніх років поживається процес «гармонізації законодавств», що безпосередньо стосується таких понять, як «монополія», «конкуренція» та «економічно вагома інформація».

Початком цього був Римський договір 1957 року, згідно з яким був створений Спільний ринок. Ст. 85 цього договору визначає: «Всі угоди між підприємствами, рішення асоціацій підприємств та узгоджені дії, які можуть впливати на торгівлю між державами та які за своєю метою чи наслідком запобігають, обмежують чи виключають конкуренцію всередині Спільного ринку, є такими, що:

- прямо чи опосередковано фіксують закупівельні чи продажні ціни, інші комерційні умови;
- обмежують чи контролюють виробництво, ринки, технічний розвиток чи інвестиції;
- розподіляють ринки чи джерела постачання;
- застосовують неоднакові умови до еквівалентних угод з іншими сторонами щодо торгівлі, чим ставлять її у не вигідне конкурентне становище;
- ставлять узгодження контрактів у залежність від прийняття іншими сторонами додаткових зобов'язань, які за суттю чи відповідно до комерційних традицій не мають ніякого зв'язку з предметами цих контрактів²⁰⁹.

Узагалі, уперше патентний закон з'явився в Англії у 1623 році. До кінця XIX століття його принципи в цілому задовольняли товарно-грошові відносини. У зв'язку з розвитком конкуренції, її жорсткістю виникла нагальна необхідність пошуку додаткових засобів підтримки змагання у сфері економіки. За рубіжні та сучасні вітчизняні економісти мають тверде переконання, що без конкуренції суспільство приречене на застій. Це означає, що конкуренція з погляду економічного розвитку країни є позитивом. Монополія обмежує конкуренцію, що є негативом. Але є ще й монополія за законом — патент. Ліквідувати патентну монополію — означає знищити стимул, поставити її над законом — це шлях до неминучих зловживань, деградація суспільства. Тому країни, що мали тривалий розвиток як демократичних принципів розбудови держави, так і повагу до комерційних засад застосування результатів науково-дослідницьких пошуків та їх результатів, дійшли цілком логічного висновку: монополію за законом потрібно гармонійно поєднати з конкуренцією на правових засадах, чинних всередині країни та таких, що відповідають міжнародним принципам.

Зважаючи на це, в Канаді, США приймають перші у світі антимонопольні (антитрестівські) закони, суть яких полягала в забороні угод на необґрунтовані обмеження торгівлі. Закони обстоювали інтереси дрібних виробників, які не мали змоги конкурувати з монополіями. Для політичної кар'єри досить було проголосити себе ворогом монополії та обіцяти домагатися її заборони. Але перевага концентрації капіталу була такою очевидною, що через різні форми та різних приводів життєздатні монополії не визнавалися порушниками закону. Це було не тільки в перші роки, а й тоді, коли політики, економісти усвідомили та визнали наявність монополістичного крену в економіці.

Протягом 40 — до кінця 80-х років XIX століття США вживали рішучих заходів щодо застосування антимонопольних норм та стали розглядати положення ліцензійних угод, керуючись «правилом резону». Воно визначило терпимість до антиконкурентних обмежень у ліцензійних угодах, якщо вони дозволяли максимізувати економічні вигоди, особливо ринкову ефективність, та посилити інноваційні процеси²¹⁰.

Згідно із Конституцією США (ст.1, розд.8) Конгрес може надавати авторам та винахідникам виключне право на визначений термін для отримання прибутку за їх розробками. Мета такого права полягає в забезпеченні наукового прогресу, а не у наданні винагороди авторам та винахідникам. Затверджене законом надання прав на інтелектуальну власність надає власникові цих прав обмежену монополію у обмін на вільне та повне розкриття ідей. Таким чином, суспільство здобуває користь із знань та розвитку науки.

Поширення знань серед людей — основне завдання охорони інтелектуальної власності, а приватна користь, що гарантується наданням прав на інтелектуальну власність, має бути збалансованою з громадським інтересом при її (власності) поширенні.

Сутність патентного законодавства США досить кардинально змінилась після прийняття поправки до Закону про патенти та торговельні марки (1980 рік, Цивільне законодавство 96-517), поправок до цього закону. По суті, ці закони надають право як невеликим, так і великим підприємствам, що працюють не для отримання прибутку, інститутам та університетам звертатися

за виключними патентами до федеральних НДДКР, а також бути власниками таких прав упродовж восьми років.

Авторське право надається Офісом авторських прав бібліотеки Конгресу США авторів на оригінальну та опубліковану роботу. Цей метод передшоджає комерційному поширенню публікацій, що містять ідеї або інформацію, але не самих ідей або інформації. (Це положення, перенесене на ґрунт України у Законі «Про авторське право і суміжні права», стало на заваді багатьом починанням тому, що в цілому законодавче поле щодо інтелектуальної власності в інформаційній сфері дуже відрізняється від аналогічного у США).

Як вважають американці, у 1990 році розпочався новий етап пошуку компромісу між конкуренцією та монополізацією. Позиція Антитрестівського комітету Мін'юсту США: «Основоположний принцип нашої політики щодо інтелектуальної власності полягає в тому, що ми ставимося до неї як до будь-якої форми власності. Інтелектуальна власність не підлягає виключенню у разі застосування антитрестівського законодавства. Обмеження цих прав жодним чином не відрізняється від прав власників іншої власності»²¹¹. При цьому у антимонопольному законодавстві увага акцентується на правах розробників та поширювачів, а також на вимогах безпеки федерального уряду.

Це набуває особливої ваги у зв'язку із зростанням значення ЗІР для результатів науково-технічних досліджень. Ноу-хау розглядається ЄС як інформація, яка є секретною, існує та ідентифікується в будь-якій формі. Правила підкреслюють, що ноу-хау як технічна інформація, що не патентується, набуває дедалі вагомішого економічного значення порівняно з інформацією, яка надає монополію (патентозахищена).

Виникає також новий клас документальних джерел, так званої сірої літератури, яка створюється переважно в комп'ютерних системах та поширюється через локальні й глобальні мережі. «Сіра література» слугує підґрунтям інформаційного забезпечення віртуальної реальності, підмножиною якої є і традиційні джерела НТІ, що не публікуються. В умовах глобальної інформатизації, усвідомлення вагомості та «економічності» статусу ЗІР діяльність інформаційних органів, що працюють з таким видом документації, набуває першорядного значення для

розробки стратегії держави, особливо щодо інформаційного забезпечення сфери НДДКР²¹².

В інформаційному суспільстві друкований документ став поступатися своєю провідною роллю. На перший план виходять так звані неоприлюднювані джерела інформації, що традиційно займали периферійне місце у сфері НТІ. Терміни «неоприлюднювані документи» та «неоприлюднювані джерела інформації» вже перестають бути адекватними тому класові документальних джерел, які становлять інформаційну базу віртуальної реальності. Тому є закономірним поширення мовного обігу терміна «сіра література», що широко використовується за кордоном. Підмножиною сірої літератури є і традиційні неоприлюднювані джерела НТІ — звіти, дисертації, описи алгоритмів та програм тощо, у тому числі і на паперовому носії.

У Російській Федерації, добре розуміючи взаємовплив інформаційного забезпечення у комп'ютерних та традиційних мережах поширення змістовних інформаційних ресурсів, зважили на доцільність створення спеціалізованої організації, до компетенції якої належить зазначене питання. Постановою Уряду РФ №950 від 24 липня 1997 року затверджене Положення про Державну систему науково-технічної інформації Російської Федерації, яке передбачає наявність спеціального державного інформаційного центру всеросійського статусу, що має комплектувати федеральний фонд неоприлюднюваних джерел НТІ та поширювати документи цього фонду серед користувачів. З 1997 року такою організацією є Всеросійський науково-технічний інформаційний центр (ВНТЩентр), що виконує згідно з положенням функції головної організації Росії з неоприлюднюваної НТІ. З урахуванням нових процесів та вимог інформатизації суспільства визнана за необхідність розробка технологічних засад розвитку на базі ВНТЩентру Федерального інформаційного центру з «сірої літератури», напрями діяльності якого охоплювали б не тільки архівування та поширення цілого спектру традиційних та нетрадиційних видів неоприлюднюваних документів, а й підтримували б і розвивали інформаційну базу систем та мереж віртуальної реальності.

У цілому такий інформаційний центр має виконувати функції інформаційного забезпечення завдань державного та науково-

го планування і регулювання процесів інформатизації та розвитку систем і мереж віртуальної реальності, їх інформаційного наповнення. В Україні функції такого центру частково могли б бути покладені на УкрШТЕІ як центр-депозитарій НДДКР та дисертацій, а також частково на Державну науково-технічну бібліотеку, яка відповідає за фонд депонованих рукописів.

В умовах глобальної інформатизації державна участь у формуванні, збереженні та поширенні «сірої літератури» як частини ЗІР набуває першорядного значення в економічній та політичній стратегії державного розвитку та проведенні її в життя. Важливість інформації в економічній галузі наочно підтверджує і приклад таких країн, як Німеччина, Японія, Південна Корея: різкий стрибок у їхньому розвитку значною мірою зумовлений масованим використанням новітньої наукової, технічної і технологічної інформації, що добувається в усьому світі.

Але якщо володіння змістовними інформаційними ресурсами створює передумови для прогресивного розвитку, то викривлення інформації, блокування процесу її одержання або впровадження хибної інформації може призвести до непередбачуваних наслідків. Найменший огріх у роботі електронних пристроїв або несанкціонований витік інформації з них можуть призвести до хаосу, банкрутства фірм, негативно вплинути на долю людей.

Безпека змістовного інформаційного ресурсу з погляду державних інтересів розглядається як важливий елемент національної безпеки. При цьому під захистом інформації розуміють систему правових, організаційних, технічних і інших дій законодавчої і виконавчої влади, державних установ країни, місцевого самоврядування, підприємств, спрямовану на збереження державної, службової, комерційної, інших видів таємниць та інформації обмеженого користування.

Законом України «Про захист інформації в автоматизованих системах» визначено, що захист інформації — це «сукупність організаційно-технічних заходів і правових норм для запобігання заподіяння шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією» (ст.1).

Можна навести чимало негативних прикладів, пов'язаних з нерозумінням важливості питань захисту інформації з боку посадових осіб. Проте сьогодні Уряд України починає вживати

комплексних заходів, для подолання цього, зокрема, розглядається питання про можливість допуску до державної таємниці осіб, які зараховані до кадрового резерву, але не мають встановленої форми допуску. Набуває особливого значення питання, пов'язане з обмеженнями в доступі до інформації при застосуванні сучасних інформаційних технологій, поширенням можливостей засобів несанкціонованого доступу і впливу на інформацію тощо.

На жаль, перебудова економічного устрою, нові умови господарювання і міжнародного співробітництва випереджають розробку і впровадження вітчизняних правових норм і організаційних заходів у сфері збереження і обігу науково-технічної інформації, а підхід до правових питань охорони об'єктів інтелектуальної власності в Україні є неповним і досить недосконалим. Ситуація ускладнюється тим, що основні відомості про об'єкти та технології у таких областях, наприклад, як оптоелектроніка, ІЧ-техніка і нині зберігаються у закритих фондах інформації, оскільки фінансувалися (до 1992 року), як правило, Комісією з питань ВПК колишнього Союзу. Звіти з науково-дослідних, дослідно-конструкторських, дослідно-технологічних розробок (НДДКТР) з оборонної тематики; описи секретних винаходів спеціалістів оборонних галузей промисловості; статті та повідомлення про результати НДДКТР були опубліковані, головним чином, у закритих науково-технічних виданнях і дисертаціях спеціалістів підприємств оборонного комплексу і нині зберігаються у спецфондах (до 1994 року — виключно російських)²¹³.

Матеріали фондів — масиви науково-технічної інформації підприємств України мають бути відповідно оцінені за ринковими критеріями. Але це можливо лише за умов вирішення низки організаційних та правових заходів, пов'язаних із питаннями промислової власності (не секрет, що далеко не всі результати таких досліджень захищені відповідним охоронним документом). Розв'язання цих питань можливе на рівні міжурядових політичних домовленостей та міжгалузевих науково-технічних виробничих рішень щодо спадковості наукових досліджень, організації спільної бізнесової діяльності, розробки критеріїв цінності змістовних інформаційних ресурсів. Сьогодні це набуває статусу національної проблеми. Час вимагає необхід-

ності виваженого, ретельного дослідження фактично нових для України законодавчих та нормативних основ сфери інформаційних відносин, оскільки держава несе вагомий фінансовий тягар, забезпечуючи зберігання інформації, віднесеної до державної та інших видів таємниці, тоді як загальносвітові тенденції інноваційного розвитку економіки потребують впровадження більш гнучкої і оперативної діючої системи розсекречення матеріальних носіїв інформації²¹⁴.

Велика кількість спеціалістів академічної, вузівської і галузевої науки останні десять років працює за програмами, які фінансуються за рахунок закордонних джерел. Маючи вагомі наукові результати і перспективи їх впровадження, вітчизняні фахівці намагаються знайти іноземні інвестиції для своєї наукової роботи: обстоюючи свої позиції в творчих конкурсах, передають закордонним партнерам не тільки результати досліджень, що ними виконувались протягом десятиліть. Тобто величезний обсяг інтелектуальної продукції витікає за кордон. Відкидаючи проблеми шпигунства і підкупу політичної та наукової еліти, відповідальних за технократичну політику держави, можна стверджувати, що таке співробітництво, вочевидь, відводить нашій державі «донорську роль». Витоку відомостей недостатньо запобігає навіть патентування винаходів.

Звичайно, в умовах ринкової економіки фірми намагаються здійснити впровадження у виробі і технологіях подвійного використання, оскільки це дає їм змогу швидко створювати конкурентоспроможну техніку та опановувати світові ринки за рахунок державного бюджету і податково-амортизаційних пільг. Більш того, така політика спонукає ланки всього ланцюга інноваційної діяльності — від вузівських вчених і талановитої молоді до інженерів і спеціалістів виробничої сфери, фірм, приватного капіталу і т.д. — впроваджувати на правах власності результати своїх досліджень. Іншими словами, визнання прав власників інформаційних ресурсів набуває в світі стратегічного значення і впливає на динаміку економічного розвитку.

За таких умов сьогодні, під час обробки та реалізації норм правового забезпечення управління у процесі функціонування системи науково-технічної інформації держави, постає вибір між двома конкуруючими правовими підходами, а саме: віднесення НТІ до сфери матеріальної або інтелектуальної власності.

У багатьох випадках виникають прикінцеві та змішані ситуації, які не охоплюються чинними нормативно-правовими актами і потребують спеціального розгляду.

З огляду на таке розуміння проблем інформаційної безпеки держави в інвестиційно-інноваційній галузі доцільно проаналізувати конкурентні переваги існуючих науково-технічних пріоритетів і законодавчо закріпити перспективи їх розвитку, не поділяючи їх на оборонні та цивільні.

Така орієнтація зумовлена і зростаючою потребою у промисловій та бізнес-інформації для багатьох підприємств, яка зараз спостерігається у всьому світі й стимулюється розширенням глобальних економічних зв'язків. У цю діяльність сьогодні активно включилися підприємства, для яких раніше, за адміністративно-розподільчої системи, така потреба не виникала, оскільки цим займалася лише невелика кількість обраних організацій зовнішньої торгівлі. На думку М. Прокоф'єва, висловлену ним на засіданні «круглого столу» 23 травня 2001 року, «...регулювання суспільних відносин, що виникають з приводу інформації з обмеженим доступом, яка не становить державної таємниці, є «білою плямою» в законодавстві України. Це зумовлено не лише відсутністю чіткого розмежування конфіденційної та таємної інформації, а й безсистемним та недбалим викладенням положень, які стосуються будь-якої інформації з обмеженим доступом, якщо вона не становить державної таємниці, непридатність відповідних норм до практичного застосування»²¹⁵. Суголосними з цими поглядами щодо проблем, пов'язаних з інформацією з обмеженим доступом, яка не становить державної таємниці, є висновки й інших учасників «круглого столу»²¹⁶. Автор цієї праці також наголошував на існуванні цієї проблеми²¹⁷, а у монографії зазначалося, що в «... в економічному, соціально-політичному та організаційно-правовому плані в Україні досі не створено логічно завершеної системи державного управління національними інформаційними ресурсами»²¹⁸.

Правові норми регулювання інформаційних відносин у демократичному суспільстві щодо таємниць та конфіденційної інформації чинне законодавство України визначає далеко не в повному обсязі. Деякі норми законів можуть неоднозначно тлумачитися або бути не зрозумілими за змістом.

Так, у ст.30 Закону України «Про інформацію» встановлено, що «громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного характеру або такою, що є предметом їх професійного, ділового, виробничого, банківського, комерційного інтересу ... самостійно вирішують режим доступу до неї, включаючи належність її до конфіденційної ...». Зміст цієї правової норми свідчить про те, що така інформація може бути як конфіденційною, так і іншою передбаченою законом таємницею. Окрім того, незрозуміло, що включається до складу «професійного, ділового, виробничого та іншого характеру». Не може бути також підставою (критерієм) для віднесення інформації до категорії конфіденційної наявність до неї «іншого інтересу» тому, що такий «інтерес» може мати й кримінальну спрямованість.

Необхідність встановлення правового режиму кожного виду інформації з обмеженим доступом передбачена фактично базовим для інформаційної сфери Законом України «Про інформацію», який передбачає, зокрема:

- забезпечення законності одержання, використання, поширення та зберігання інформації (ст.14);
- створення загальної системи охорони інформації (ст.6);
- установлення режиму доступу до інформації на підставі порядку, передбаченого правовими нормами (ст.28);
- розподілення інформації за режимом доступу на відкриту інформацію та інформацію з обмеженим доступом (ст.28);
- віднесення інформації до категорії таємних відомостей, порядок і терміни обнародування таємної інформації тільки на підставі відповідних законів (ст.30);
- регулювання законодавством права власності на інформацію (ст.38) та охорони цього права законом (ст.45);
- установлення відповідальності за порушення законодавства України про інформацію (ст.47);
- гарантування інформаційного суверенітету України на підставі забезпечення виключного права власності України на інформаційні ресурси, що формуються за рахунок коштів державного бюджету, встановлення режиму доступу інших держав до цих ресурсів та використання їх на основі рівноправного співробітництва з іншими державами (статті 53, 54).

Наведене свідчить про те, що правові норми Закону України «Про інформацію» передбачають розвиток інформаційного законодавства на підставі впровадження на рівні законів правових норм щодо вдосконалення правового режиму різних видів інформації з обмеженим доступом. Такі правові норми введені в дію у повному обсязі лише стосовно державної таємниці.

Відповідно до світової практики нормотворення, вітчизняного досвіду та результатів досліджень із цих питань до системи правового режиму інформації з обмеженим доступом доцільно включити такі правові норми щодо регулювання суспільних інформаційних відносин, а саме:

а) визначення науково і юридично обґрунтованих понять:

— конфіденційна інформація (інформація професійного, ділового, виробничого характеру, та інтерес до неї фізичних та юридичних осіб, а також зміст конфіденційної інформації про особу);

— інша передбачувана законодавством таємниця (службова, військова, комерційна, медична, адвокатська, досудового слідства, оперативно-розшукова, дорадчої кімнати, судова, страхування, нотаріальних дій, таємниця особистого життя та ін.);

б) перелік видів інформації, що становить іншу передбачувану законодавством таємницю та відомості, які можуть бути віднесені до конфіденційної інформації, а також переліки відомостей, які заборонено відносити до інформації з обмеженим доступом, що не становить державної таємниці. Цей розділ повинен також містити правові норми, які визначають критерії та підстави віднесення інформації до відповідної категорії відомостей;

в) визначення порядку встановлення режиму доступу до цієї інформації, надання матеріальним носіям такої інформації відповідного грифу обмежень та строків дії встановлених обмежень;

г) встановлення основних організаційно-правових, інженерно-технічних (за необхідності, криптографічних) заходів захисту інформації, які відповідали б встановленому рівню обмежень доступу (режиму конфіденційності);

д) визначення юридичних норм щодо права власності на інформацію й механізмів гарантування цього права;

е) встановлення правових норм щодо відповідальності суб'єктів інформаційної діяльності за порушення вимог інфор-

маційного законодавства з визначенням кримінальних, адміністративних і цивільно-правових санкцій.

Таким чином, основи правового режиму інформації — це установлені законодавством правові норми регулювання суспільних інформаційних відносин щодо впровадження ступенів відкритості (закритості) інформації, порядку і правил віднесення відомостей до категорії з обмеженим доступом, забезпечення режиму секретності (конфіденційності), гарантування права власності на інформацію та правового захисту інтересів суб'єктів інформаційної діяльності.

Формування СНІР щодо реєстрації, накопичення і зберігання, поширення та використання інформації з обмеженим доступом обов'язково мають передбачати заходи забезпечення режиму секретності (конфіденційності) інформації, що підлягає охороні, відповідно до порядку та правил, встановлених чинним законодавством України.

Важливою складовою правового режиму і ключовим питанням системи охорони інформації є режим доступу до неї. Відповідно до чинного законодавства за режимом доступу інформація поділяється на відкриту та з обмеженим доступом²¹⁹. У ст. 28 закону визначено і зміст поняття «режим доступу до інформації» як передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації.

Закон України «Про державну таємницю»²²⁰, визначаючи зміст заходів щодо режиму доступу, включає до нього такий етап, як виготовлення інформації, що становить державну таємницю, та її матеріальних носіїв. Це дуже важливий аспект правової норми, що регламентує порядок і правила режиму доступу, які мають конче виконуватися в процесі формування ЗІР, починаючи з етапу створення (виготовлення) інформації з обмеженим доступом.

Ще одним важливим аспектом правової норми щодо правового режиму інформації є відсутність поділу інформації за ознаками права власності. Тобто власник має право установлення режиму доступу до інформації з обмеженим доступом, що йому належить, але в межах, визначених законодавством.

Сучасні визначення категорій інформації за режимом доступу можуть бути зведені до таких.

Відкрита інформація. Як визначено чинним законодавством України, доступ до такої інформації забезпечується шляхом:

- систематичної публікації в офіційних друкованих виданнях (бюлетенях, збірниках);
- поширення її у засобах масової інформації (комунікації);
- безпосереднього її надання заінтересованим громадянам, державним органам та іншим суб'єктам як безпосередньо, так і за запитами.

Обмеження права на одержання відкритої інформації забороняється законом²²¹.

Конфіденційна інформація. Право доступу до такої категорії інформації надається власником цієї інформації²²². Залишається неврегульованим у правовому і організаційному плані порядок доступу до конфіденційної інформації про особу, що збирається й накопичується державними органами для виконання функцій державного управління.

Таємна інформація, що не становить державної таємниці. Доступ до такої інформації, яка є власністю держави, надається керівниками державних органів, підприємств, установ і організацій та керівниками їх структурних підрозділів"*.

Державна таємниця — це відомості, які є власністю держави. Відповідно до чинного законодавства доступ до державної таємниці надається дієздатним громадянам України, яким надано допуск до державної таємниці та які потребують його за умовами своєї службової, виробничої, наукової чи науково-дослідної діяльності або навчання²²⁴.

Для роботи з секретною *інформацією*, що має ступені секретності «особливої важливості», «цілком таємно», «таємно», встановлено допуск форми 1; зі ступенями секретності «цілком таємно» і «таємно» — допуск форми 2; із ступенем секретності «таємно» — допуск форми 3²²⁵.

. Право надання доступу до конкретної секретної інформації та її матеріальних носіїв мають тільки перші керівники державних органів, підприємств, установ і організацій²²⁶.

Концептуальні проблеми раціонального використання змістовних інформаційних ресурсів України (див. розділ 1) передбачають, що накопичені суспільством знання, наукові досягнення мають працювати передусім на розвиток економіки держави та забезпечення її національної безпеки. Не визначивши на рівні

актів законодавства правових норм регулювання відносин, пов'язаних з захистом інформаційних ресурсів, не встановивши компетенції і не забезпечивши скоординованих дій з цих питань державних органів та інших суб'єктів, що діють в інформаційній сфері, неможливо, без збитків для суспільства і держави, здійснювати формування, розвиток і використання інформаційних ресурсів. Недооцінка важливості цього, прорахунки перших років, створили правову дисгармонію, наслідком якої є те, що до цього часу в Україні не закінчено створення логічно завершеної системи захисту інформаційних ресурсів.

Сьогодні стало цілком зрозуміло, що зміна тоталітарної системи засекречування загальною системою відкритості, зволікання щодо формування і застосування ефективно діючої національної системи державної таємниці негативно впливала і продовжує негативно впливати як на забезпечення національної безпеки, трансформацій в економіці, так і на матеріальний добробут громадян.

Як зазначалося, чинне законодавство України не дає повного юридичного визначення понять «інформація», «інформаційні ресурси». Це призвело до того, що в кримінальному та адміністративному праві відсутні науково обґрунтовані юридичні тлумачення широкого спектру правопорушень в інформаційній сфері, а галузеві інститути законодавства не в повному обсязі передбачають правові санкції за ці правопорушення.

Досвід державного будівництва за минулі десять років змушує зробити висновки про те, що організаційно-правова система, інформаційне законодавство неспроможні ефективно забезпечити захист як права громадян на інформацію, так і власне змістовну інформацію, що підлягає охороні з боку держави. В організаційній структурі державних органів та інших суб'єктів, що діють у сфері захисту інформаційних ресурсів, відсутні деякі ланки, а ще деякі — з об'єктивних і суб'єктивних причин — не працюють.

Характерною ознакою демократичного розвитку, навіть розвинутих країн, є активний пошук шляхів і розробка комплексних програм входження в інформаційне суспільство. Як правило, такі програми передбачають комплекс заходів, спрямованих на розв'язання ряду таких проблем:

- визначення державної стратегії й політики щодо використання переваг інформаційного суспільства для соціально-економічного розвитку і забезпечення національної безпеки;

- формування і розвиток інформаційного законодавства як правового фундаменту інформаційного суспільства;

- комплексне створення національних інформаційних інфраструктур, координація діяльності органів державної влади, державних і недержавних структур у сфері інформатизації;

- внесення, з урахуванням нових завдань, докорінних змін у діяльність інститутів забезпечення національної безпеки, воєнну стратегію і підходи до питань оборони країни;

- захист суспільства від недоброякісної інформації та дезінформації;

- захист національних ЗІР від несанкціонованого доступу правовими, організаційними, технічними, криптографічними заходами і засобами;

- розвиток нових видів і форм діяльності в інформаційних системах і мережах;

- запобігання і боротьба з новими видами злочинів у інформаційній сфері та інформаційно-телекомунікаційних системах; координація діяльності з цих питань з відповідними міжнародними організаціями.

Характеризуючи національну систему охорони державної таємниці, її відповідність новим умовам господарювання та постіндустріальному етапу розвитку, треба підкреслити, що законодавче і нормативно-правове забезпечення і в цій, найбільш урегульованій сфері захисту інформаційних ресурсів, ще недостатнє, не враховує важливих процесів і змін, які відбуваються у суспільстві. Відсутність науково обґрунтованих політичних і соціально-економічних критеріїв і методик віднесення інформації до державної таємниці стала визначальною проблемою для цієї сфери діяльності.

На початковому етапі формування системи охорони державної таємниці колишнім Держкомсекретів України були розроблені і введені в дію «Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення інформації до державної таємниці та ступеня їх секретності». Запропонований у цих рекомендаціях метод експертних оцінок дав змогу приблизно визначити величину економічної

шкоди внаслідок розголошення або втрати відомостей, які віднесені чи мають бути віднесені до державної таємниці.

Однак сьогодні, коли розвиток держави, перехід до ринкової економіки, розвиток міжнародних відносин створюють нові правові умови в інформаційній сфері, а змістовні інформаційні ресурси набувають ознак товару, метод «приблизного визначення в умовних одиницях» підстав для віднесення інформації до державної таємниці та оцінки шкоди у разі втрати або розголошення цієї інформації потребує суттєвої корекції.

Залишається недосконалим юридичне регулювання відносин, пов'язаних з правом власності на об'єкти промислової власності та ті, що охороняються авторським правом. Немайнові активи сьогодні є предметом зацікавлення іноземних фірм, проникнення яких на вітчизняний ринок зумовлене лише скуповуванням охоронних документів на об'єкти промислової власності (ОПВ). Власник ОПВ використовує недоліки їхньої правової охорони для завоювання та освоєння ринку збуту своїх товарів і технологій, перемагаючи в боротьбі за отримання прибутків, але не шляхом конкуренції технологій.

Окремому розгляду підлягають питання захисту державної таємниці в процесі міжнародного наукового і науково-технічного співробітництва. Механізм вирішення цих питань недосконалий, для їх розв'язання необхідно подолати діючі в Україні дві тенденції, а саме: перша — максимальне засекречування як метод зберегти для держави унікальні наукові здобутки; друга — наука має бути відкритою і не повинна засекречуватися. Перша тенденція спрямовує за межі розумної закритості, друга — за межі розумної відкритості. Тому потрібен посередник у вигляді ефективно діючого правового механізму та відповідних організаційних заходів держави.

На державному рівні визначені підходи до Національної програми інформатизації. Водночас її завдання здійснюються в умовах недостатньо керованих державою процесів. Сьогодні перевага у виготовленні технічних засобів обробки інформації та засобів зв'язку надається іноземним виробникам, у державі переважає тенденція створення ІТС на основі архітектури відкритих систем. Фактично ігноруються вимоги чинного законодавства (Закону України «Про державну таємницю» (ст.7), постанови Кабінету Міністрів України від 15 червня 1994 року № 414 (п.2)

«Про віднесення витрат на створення систем захисту інформації до собівартості виконання програм і проектів інформатизації»). Впроваджені в Україні цифрові комутаційні станції іноземних фірм дають можливість дистанційно, з будь-якої відстані, міжнародними каналами зв'язку не тільки знімати інформацію з абонентів мереж, а й блокувати їх, виключати станції тощо. Все це блокує розвиток ІТС для обробки і поширення інформації з обмеженим доступом та створює передумови не лише для витоку закритої інформації, а й для блокування мереж зв'язку державного управління.

Актуальною стає проблема концептуальної неузгодженості правових норм, що регламентують порядок створення і функціонування підрозділів, які забезпечують захист інформації від витоку технічними каналами, що раніше мали назву підрозділів протидії іноземним технічним розвідкам.

У державі діє низка нормативно-правових документів, які передбачають обов'язкову наявність таких підрозділів і служб. Водночас Закон України «Про захист інформації в автоматизованих системах», прийнятий у липні 1994 року, який є основним законом системи ТЗІ, в ст.15 проголошує, що «у державних установах та організаціях *можуть створюватись* підрозділи і служби, які організують роботу, пов'язану із захистом інформації, підтримки рівня захисту інформації в АС»²²⁷. В умовах сформованого на той час залишкового принципу фінансування робіт з охорони державної таємниці та ТЗІ керівники державних органів та організацій, керуючись положенням, що вони «можуть створювати» вказані підрозділи і служби, наприкінці 1994 року закінчили їх ліквідацію, а в деяких випадках скоротили до одиничних осіб.

Виконання робіт і послуг з технічного захисту інформації в державі необгрунтовано покладене лише на суб'єктів підприємницької діяльності. Не заперечуючи проти діяльності цих суб'єктів на підприємствах вільного сектору економіки, треба підкреслити, що у правовому аспекті використання науково-технічного і виробничого потенціалу, що належить до сфери управління державних органів, має стати обов'язковим. Створення на базі можливостей державних науково-виробничих центрів, підрозділів і служб з виконання робіт по захисту інформації від витоку технічними каналами, не тільки зменшило б

переливання і бюджетних коштів до комерційних структур, а й підвищило б об'єктивність оцінки реального стану технічного захисту інформації в Україні.

Транснаціональні інформаційно-телекомунікаційні системи ліквідовують географічні і геополітичні кордони. В інформаційному просторі починають діяти п'ять суб'єктів інформаційних відносин: створювач, постачальник, передавач, розподільник і користувач інформації. Крім того, є ще власник інформаційних систем і комунікацій. Усі ці суб'єкти права можуть бути представниками різних країн, де діють різні правові норми, у тому числі і ті, що регламентують відповідальність за порушення прав суб'єктів інформаційних відносин. Це нова ситуація у сфері міжнародних відносин, що тільки окреслюється, потребує комплексного аналізу і наукового обґрунтування підходів до її правового врегулювання.

В сучасних умовах набуває політичного значення необхідність розробки і впровадження ефективно діючих правових механізмів захисту прав власника і володаря інформаційних ресурсів, об'єктів інтелектуальної власності з урахуванням як внутрішніх, так і міжнародних аспектів. Основою для розробки таких механізмів національного законодавства є конституційне право та вдосконалення інститутів права власності, патентного і авторського права. Стосовно регулювання міжнародних інформаційних відносин основою має бути теорія і практика інституту римського права власності. До того ж особливо важливим як для національного законодавства, так і міжнародного права є забезпечення власникові і володареві ЗІР можливості отримання відповідних прибутків та ефективного захисту цього права.

Прогресивним кроком на шляху до впровадження сучасних інформаційних технологій у різноманітні сфери діяльності суспільства є Указ Президента України від 31 липня 2000 року № 928 «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні». Це не тільки можливість розширення доступу до світових інформаційних ресурсів, а й крок, у широкому плані, на шляху до світового розподілу праці. Це можливість включення українського інтелектуального потенціалу до транснаціональних структур високотехнологічних

виробництв. Адже в умовах інформаційно-технологічної революції одним із важливих показників рівня розвитку держави є експорт ЗІР, наукових і технологічних рішень.

Відомо, що над розробкою заходів забезпечення реалізації вимог Указу Президента України проводиться серйозна робота. Водночас, враховуючи сумнозвісні уроки впровадження і наслідків виконання Національної програми інформатизації, а саме: «Спочатку виконуємо проект створення системи, а потім думаємо як захищати те, що в ній циркулює і накопичується», було б доцільним передбачити у загальному комплексі концептуальні, організаційні, правові заходи превентивних дій щодо інформаційної безпеки, спрямованих на:

- захист суспільства від недоброякісної інформації, дезінформації та можливої інформаційної експансії з боку інших країн;
- захист національних інформаційних ресурсів від несанкціонованого доступу, їх пошкодження та знищення;
- забезпечення скоординованих дій України з відповідними міжнародними організаціями з питань боротьби з новими видами злочинів в інформаційній сфері та інформаційно-телекомунікаційних системах.

Важливим елементом забезпечення реалізації державної інформаційної політики та захисту інформаційних ресурсів є наявність у державі організаційної функціональної структури державних органів, інших суб'єктів, що діють у інформаційній сфері.

В Україні на рівні актів законодавства та відповідних державних рішень визначено державні органи, які забезпечують реалізацію державної інформаційної політики, а саме:

- стосовно засобів масової інформації та видавничої сфери — Державний комітет інформаційної політики, телебачення і радіомовлення*;

* Згідно з Указом Президента України від 31 січня 2003 року Державний комітет інформаційної політики, телебачення і радіомовлення України перейменовано на Державний комітет телебачення і радіомовлення. Як наголосив голова Держкомтелерадіо І. Чиж, «наша структура дозволяє, крім телевізійної та радіої складової, забезпечити здійснення інформаційної політики та управлінських функцій у сфері друкованих засобів масової інформації, книгодрукування та видавничій сфері» («Урядовий кур'єр» від 6 лютого 2003 року).

— у сфері, пов'язаній з державною таємницею, захистом державних інформаційних ресурсів у мережах передачі даних, криптографічним і технічним захистом інформації, — Служба безпеки України;

— з питань інформатизації — Державний комітет зв'язку та інформатизації України.

У процесі реформування державних органів втрачено функцію державного управління розробкою і впровадженням організаційних, нормативно-правових заходів, координації і контролю за реалізацією державної політики у сфері захисту інформаційних ресурсів з обмеженим доступом, що не становить державної таємниці. Це негативно позначається на повноті даних загальнодержавної системи реєстрації національних інформаційних ресурсів. Згідно з рішеннями Уряду України в державі створена певна структура реєстрації та зберігання результатів відкритих науково-технічних програм і проектів. Ця система включає Український інститут науково-технічної і економічної інформації (УкрІНТЕІ), державні науково-технічні бібліотеки та регіональні центри науково-технічної і економічної інформації. Частково така реєстрація провадиться і за розробками закритої тематики (в галузевих установах та УкрІНТЕІ).

Залишається невизначеною державна система накопичення, моніторингу і поширення інформаційних ресурсів, що містять відомості, віднесені до державної таємниці, іншої інформації з обмеженим доступом.

Не встановлено і порядок загальнодержавної реєстрації інформаційних ресурсів, що створюються в процесі діяльності Верховної Ради України, Адміністрації Президента України, Ради національної безпеки і оборони України.

Відсутній механізм реєстрації і поширення в загальнодержавних інтересах інформації, яку отримує Україна в процесі її міжнародної діяльності.

У державі немає єдиних уніфікованих нормативів (стандартів), методичних, організаційних, технологічних принципів формування, розвитку і поширення ЗІР. Кожне міністерство, інші державні органи створюють для своїх потреб внутрішньовідомчі інформаційні ресурси без узгодження технології їх формування. Усе це створює умови, за яких гальмується формування на-

ціонального інформаційного простору, адекватного інтелектуальному потенціалу суспільства.

За таких обставин розвиток національної інформаційної інфраструктури (ПФС) доцільно здійснювати з урахуванням вимог чинного законодавства щодо захисту інформаційних ресурсів, які підлягають охороні з боку держави.

У майбутніх умовах інформаційного суспільства є проблематичним розраховувати на високу ефективність захисту інформації, що підлягає охороні з боку держави, з одночасним утвердженням свободи слова у зв'язку з недостатньою правовою культурою і законослухняністю громадян, у тому числі й пов'язаною з мас-медіа.

Варіантом розв'язання цих питань може бути включення до навчальних планів підготовки спеціалістів з вищою освітою такої складової, як інформаційна безпека. Знання і розуміння правових норм, що регулюють відносини в інформаційній сфері, своїх прав і обов'язків, дотримання конфіденційності ділових, виробничих та інших відносин — мають стати ознакою правової інформаційної культури громадянина.

Вирішення цього питання на практиці, на жаль, не підкріплюється відповідними заходами з боку держави. У загальноосвітніх програмах недостатньо місця відведено вивченню цих питань. Закони і підзаконні акти публікуються лише в окремих державних виданнях. Державні програми радіо і телебачення обмежуються тільки короткими повідомленнями про прийняті закони, окремі підзаконні акти та інші державні рішення.

Світова практика має багатий досвід розв'язання цих питань. У розвинутих країнах кожний солідний засіб масової інформації, у тому числі так звані незалежні та опозиційні, вважають своїм обов'язком публікацію будь-яких актів законодавства, якщо вони стосуються прав і обов'язків громадян.

\ Держава зобов'язана допомогти «незалежним» засобам масової інформації (ЗМІ) досягти цивілізованого розуміння поняття незалежності ЗМІ. Вони можуть бути незалежними від влади, від соціально-політичних угруповань, але не можуть бути незалежними від власного народу. Це один аспект проблеми, а другий полягає в тому, що доцільно повернути до цієї проблеми обличчям державні ЗМІ.

З урахуванням нашого трохи більш як десятилітнього суспільного досвіду побудови демократії та світової практики перший крок має полягати в розробці і впровадженні заходів, спрямованих на створення логічно завершеної системи правового регулювання та організаційного забезпечення захисту національних інформаційних ресурсів, що підлягають охороні з боку держави. Важливою складовою інформаційних ресурсів є державна таємниця та інші передбачені законодавством таємниці.

2.3.2. Ринкові форми інформаційного обігу та їх правове забезпечення

Розбудова державності в Україні швидко просунулася на шляху демократизації до рівня, який дає змогу ініціювати вступ до Європейського Союзу, визначати послідовність свого розвитку на засадах економічної ефективності.

Як свідчить досвід розвинутих країн світу, формування ринкових економічних відносин та структурна перебудова економіки нерозривно пов'язані зі зміною ролі державного управління як за складом, так і за напрямками своєї дії. Поряд із цим відбувається процес становлення інформаційного обігу у вигляді обігу інформації як самостійної гілки суспільного виробництва, ринкова форма якої має стати однією з головних засад функціонування ринкової економіки в цілому.

У процесі суспільно-економічної трансформації сфера обігу, у тому числі інформаційного, за результатами будь-якої науково-технічної діяльності, набуває нових видів та форм. Виникає ринок технологій, який, на думку автора, можна визначити як систему взаємовідносин споживачів технологій (їх об'єктів) та/або конкуруючих між собою постачальників цих об'єктів, спрямованих на задоволення суспільних і державних потреб у відповідних технологіях, їх об'єктах та продукції, виготовленої з їх застосуванням.

Однак слід зауважити, що з суто управлінських позицій ринок в епоху науково-технічної революції виявляється вельми недосконалим інструментом, фактично непридатним для регулювання цін на більшість видів сучасної продукції, тому що класичний ринковий механізм дає змогу виконати функцію визначення правильної ціни товару, яка дійсно відповідає його

вартості, лише за наявності великої кількості незалежних покупців, спроможних здійснити таку велику кількість покупок, щоб у процесі визначення ціни спрацював закон великих чисел; наявності достатньої кількості дійсно незалежних продавців (для унеможливлення встановлення монопольної ціни); і досить тривалого існування товару на ринку у своєму незмінному вигляді (тобто без поліпшення його споживчих властивостей). Тому на практиці ринковий метод регулювання ціни (протилежний планово-директивному методу — метод регулювання з вільною грою цін), особливо ціни на науково-технічну продукцію, ноу-хау, новітні технології тощо, перетворюється в ніким не регламентований механізм взаємодії між продавцем і покупцем з усіма наслідками, які з цього випливають. Так, у багатьох наукових дослідженнях визначаються та класифікуються види обігу за формами розрахунків, сферою діяльності, територіальними ознаками, відповідно до різноманіття об'єктів. При цьому функції обігу за ринкових умов набувають якісно нового змісту та є зумовленими структурною перебудовою власне економіки. Функція інформаційного супроводження (від етапу створення продукції до етапу споживання чи впровадження) поєднана та визначальним чином залежить від змін у власності. Виконуючи роль ланки сполучення, ця функція починає діяти за умов, коли єдина державна власність на змістовний інформаційний ресурс (результати діяльності), інформаційні системи (обробка, зберігання, способи надання відомостей), виробничо-господарську інфраструктуру (інформаційні центри та служби, підрозділи) поступаються великій кількості приватних чи недержавних власників, а власність розглядається як інституціональна основа інформаційного обігу. Процеси приватизації, реструктуризації у свою чергу мають наслідком формування реальних власників, що є суб'єктами сфери обігу та стають організаційним підґрунтям останнього, оскільки наявність приватної власності економічно та юридично забезпечує вільне використання та привласнення створюваних інформаційних продуктів та послуг.

Включення до сфери інформаційного обігу кінцевих продуктів відкриває нові можливості для формування власників фінансового капіталу, створення конкурентного середовища, забезпечення ринкової форми обігу результатами кінцевої діяльності. На даному етапі суспільно-економічної трансформації

в Україні ще не сформовані умови, за допомогою яких відтворюються і панують відносини та зв'язки ринкової форми обміну. Це стосується завершення процесу приватизації, забезпечення свободи підприємництва і вибору, реалізації особистого інтересу як головного мотиву діяльності, вільного доступу до економічних ресурсів, інформації та ринків збуту.

Однак власне нові соціально-економічні засади передбачають найістотнішою умовою свого існування довготривалість перспективи ініціативної економічної діяльності, її законодавчі гарантії. Тобто нові форми господарювання можуть успішно розвиватися лише за наявності юридичних гарантій від неправових посягань з боку держави, юридичних, фізичних осіб на власність, вільну конкуренцію, право передачі (успадкування) та інші права, які забезпечували б як економіко-правовий статус виробника чи підприємця, так і право на володіння, розпорядження, користування, що є основними складовими забезпечення права власності.

Стосовно інноваційного процесу роботи зі створення і освоєння нового продукту чи технології, тобто науково-інноваційні роботи, є збитковими. Тому при побудові інноваційної стратегії цього циклу державою мають передбачатися певні економічні чинники у системі оподаткування, кредитування, можливостях бюджетного фінансування тощо²²⁸. Процеси ж реалізації інновацій є переважно прибутковими. Беручи до уваги, що інноваційні підприємства, які самостійно розробляють і реалізують новий продукт, мають постійно працювати над його вдосконаленням і нести відповідні збитки по кожному новому продукту, норма їх прибутків є значно нижчою, ніж на підприємствах, що займаються реалізацією нововведень. Крім того, інновації, пов'язані з розробкою і впровадженням нововведення, мають тривалий цикл перебігу, високий рівень невизначеності та ризику, особливий механізм ринкової реалізації, де левову частку роботи становить опрацювання інформації. Іншими словами, врегулювання збалансованості між інформаційними процесами науково-інноваційного та виробничо-комерційного циклів у сучасних умовах також залежить і від чіткого організаційно-правового механізму реалізації державної інноваційної політики. Ось чому при розробці стратегії інноваційного розвитку держа-

ви необхідно урахувати роль та значення інформаційної складової такого процесу.

Зовнішньоекономічні зв'язки у процесі інтеграції України у світове господарство також охоплюють сферу інформаційного обміну, передусім внутрішньогалузевого. Міжгалузевий інформаційний обмін має тенденцію до деякого скорочення тому, що вихід на прямі економічні зв'язки між підприємствами поглибив (на ринковій основі) обмінні зв'язки, коли у сферу співробітництва прийшли самі товаровиробники. Процес трансформації від командно-адміністративних методів регулювання до ринкових вимагає і адекватних форм інформаційного обміну, їх правової визначеності.

Розвитку внутрішньогалузевого ринку продукції, товарів передують інформаційний обмін, а йому в свою чергу передують досягнення, насамперед науково-технічні, що дають змогу сформувати цей внутрішній галузевий ринок. Але, що собою являє науково-технічна продукція в її описовому стані: частиною ЗІР чи складовою інтелектуальної власності (ІВ), особливо коли остання має вигляд звіту про виконання НДДКР?

Сьогодні в будь-якому договорі на створення науково-технічної продукції є розділ, де стверджується, що «...виключне право при використанні ІВ, яка створена за договором, належить виконавцю та замовнику, обсяг прав та обов'язків сторін оформляється угодою між ними та за необхідності захищається охоронними документами»²²⁹. Для об'єктів, що не мають офіційного охоронного оформлення (наприклад, НДДКР, виконані за рахунок бюджету — звіти, дисертації, описи алгоритмів та програм, науково-технічні розробки типу ноу-хау), документами, які підтверджують їхній правовий статус, можуть стати угоди на створення та передачу науково-технічної продукції, котрі власне й доводять факт створення цього об'єкта.

Справді, споживчі товари та послуги ґрунтуються на досягненнях фундаментальних наук та прикладних НДДКР, створених творчою працею окремих людей, які могли б у силу особливостей власного розвитку, освіти, набутого досвіду та фахового рівня створити те, чого до них у природі та суспільстві не було, принаймні, зафіксованим. Але проблема авторства та права на результат науково-технічної діяльності, незважаючи на її досить широке законодавче охоплення (постанови уряду, укази

Президента, законодавчі документи та підзаконні нормативні правові акти, керівні та інструктивні матеріали тощо), досі реально в Україні (та й у країнах СНД) не розв'язана, а відповідна ІВ залишається «позагосподарською» і практично безконтрольною, і що ще гірше — використовується від імені держави як роботодавця на правах безвідплатної виключної ліцензії на використання такого об'єкта. Тут можуть бути наведені різні схеми надання технологій як об'єктів інтелектуальної власності, наприклад: при виконанні спільного проекту; при впровадженні у виробництво довгострокових стратегічних розробок; при впровадженні розробки, яка не була своєчасно реалізована за браком коштів; при вкладанні коштів у дослідження з високим ступенем ризику, але такого, що має загальнодержавне значення тощо (детальніше — у п.1.3).

Як зазначалося²³⁰, з орієнтацією на ринкові відносини використання ЗІР перестало бути безоплатним. Цим зумовлено введення змін і нових положень у методичні і нормативно-інструктивні, законодавчі документи, що фіксують статус інформації як товару та визначають правовий режим її використання у вигляді об'єкта ІВ. Тому проблема гармонізації інтересів виконавця, суб'єкта господарської (підприємницької) діяльності, та державного замовника щодо володіння, користування та розпорядження правами власності на результати інтелектуальної діяльності (винаходи, корисні моделі, промислові зразки, об'єкти авторського права тощо), створені в рамках договорів, що фінансуються за рахунок коштів державного бюджету або інших спеціальних державних фондів, які також стосуються продукції військового, спеціального та подвійного призначення, залишається надзвичайно актуальною²³¹.

Входження України до світового співтовариства як самостійного суб'єкта міжнародних відносин спонукає її діяти за нормами, що прийняті у ньому, пристосовувати до них свої правові положення. Проблема ускладнюється ще й тим, що документальні фонди за результатами науково-технічної діяльності, створені до 1992 р. і які не втратили свого значення і на цей час, є національною власністю або власністю РФ за визначенням²³², а тому питання їх використання набувають статусу міжнародних.

Зазначимо, що кооперація як форма міжнародного поділу праці, зокрема у сфері високих технологій як найбільш «одержавлених», включає²³³:

- взаємний обмін науково-технічними досягненнями та науково-виробничим досвідом;
- співробітництво в галузі НТІ, патентної справи та винахідництва;
- взаємні консультації з основних питань науково-технічної та технологічної політики;
- спільне розв'язання наукових, науково-технічних та науково-виробничих проблем;
- придбання та продаж ліцензій, ноу-хау, спільні випробування;
- спільне виробництво, кооперацію поставок у межах ліцензійних угод;
- розподіл виробничих програм.

Таким чином, правові положення стосовно можливості використання ЗІР за результатами науково-технічної діяльності стосуються інтересів таких рівноправних власників (вони ж є і споживачами) інформації, як держава, окремі юридичні та фізичні особи. Відносини між цими суб'єктами володіння регулюються нормами практично всіх видів права: цивільного, адміністративного, трудового, міжнародного, а у випадку виникнення конфліктів чи настання небезпечних наслідків — кримінальним законодавством або правилами арбітражу.

Відсутність в Україні цілеспрямованої політики з формування та використання ЗІР за результатами науково-технічної діяльності як єдиного стратегічного ресурсу держави веде до того, що в багатьох випадках ці процеси регулюються відомчими нормативними документами, що часто мають на меті різні цілі, які мають відомства на використання науково-технічного продукту за результатами дослідницької або впроваджувальної діяльності, що фінансується ними. Як наслідок, виникає порушення структури інформаційного ринку України, що вже став набувати цивілізованих форм. Характерною є об'єднана опозиція Державної комісії з питань оборонно-промислового комплексу України, Міністерства промислової політики України (яка була озвучена їх офіційними доповідачами на п'ятому галузевому семінарі «Проблеми введення об'єктів інтелектуальної власності в госпо-

дарський обіг та шляхи їх розв'язання» (16 жовтня 2001 року)²³⁴) і Міністерства оборони України до Міністерства освіти і науки України. У дискусії щодо проекту Закону України «Про внесення змін до Закону України «Про власність» в редакції Міносвіти і науки України (розробник проекту Державний департамент інтелектуальної власності)²³⁵, що спонтанно виникла перед закриттям семінару, особливо чітко окреслились позиції сторін, які засвідчують *принципові розбіжності різних міністерств і відомств з питань підходів щодо визначення ефективного власника прав на ОІВ*²³⁶.

Якщо Міносвіти і науки України бачить державу як суб'єкта права у випадку створення ОІВ при виконанні робіт за договорами (контрактами), фінансованих за рахунок коштів державного бюджету, якщо цей об'єкт належить до сфери державної безпеки або, якщо держава повністю бере на себе фінансування створення та введення в господарський обіг такого об'єкта, то опоненти вважають за можливе внести більш радикальні зміни як до Закону України «Про власність», до ст. 18 Закону України «Про підприємства в Україні», так і до інших законів, щоб на законодавчому рівні зобов'язати виконавця передавати права власності на розроблені ОІВ без будь-яких договірних умов.

Оскільки державне замовлення є сьогодні найбільш поширеною формою участі наукових організацій та підприємств у розробці принципово нових технологій, техніки і матеріалів і надає гарантії забезпечення не тільки фінансовими, а й матеріально-технічними засобами, передбачає гарантований збут продукції, виготовленої відповідно до держзамовлення, питання власника цієї продукції та її інформаційної складової набуває першорядного значення.

Не викликає жодних заперечень, що формуванню державної контрактної системи як механізму фінансування держзамовлення на виконання ДНТП* мають «передувати розробка та прийняття відповідних законів, нормативних документів, які регламентують діяльність та юридичну відповідальність органів-замовників та організацій-виконавців, типових документів та процедур укладання контрактів»²³⁷. Важливим моментом, що

підвищує відповідальність окремих виконавців, є право держави припиняти контракт в односторонньому порядку за рішенням замовника програми (проекту)²³⁸. Звичайно, у контрактній системі передбачаються економічні санкції, госпрозрахункова відповідальність організацій-виконавців за «несвоєчасне, неякісне виконання завдань ..., недосягнення передбачених програмою цільових показників, за неефективне використання ресурсів або використання їх не за цільовим призначенням», а також штрафні санкції. Для органів управління програмою (за прямим договором з державним органом, наприклад міністерством) передбачаються «економічні санкції ... на випадок несвоєчасного матеріально-технічного, інформаційного та іншого забезпечення». Іншими словами, такий механізм нібито забезпечує створення науково-технічної продукції, яка не завжди є патентозахищеною, але завжди має визначену ринкову цінність та визначений кошторис. Гарантії ж збуту надає замовник-власник створеного продукту, тобто державний орган, який не має права займатися будь-якою іншою діяльністю, окрім тієї, для якої він був створений²³⁹. Зокрема, він не може займатися госпрозрахунковою діяльністю, і тому незрозуміло, хто та на яких засадах має впроваджувати або збувати науково-технічну продукцію (за держзамовленням) чи вимагати накладання «економічних санкцій» на такий державний орган за неналежне виконання умов прямого контракту.

До державного контракту вписуються пункти, які «зв'язують руки» не тільки виконавцеві, а й посереднику (якщо він визначений у тому ж таки контракті), який займається комерціалізацією НДДКР. Зокрема, у технічному завданні на виконання дослідження* є пункт «Зобов'язання сторін із забезпечення охорони прав на створені об'єкти інтелектуальної власності», в якому:

— об'єкт ІВ — це «комплект науково-технічної документації, підготовлений Виконавцем відповідно до вимог та умов Договору»;

— об'єкт промислової власності — «використані у комплекті науково-технічної документації винаходи, промислові зразки,

* Державна науково-технічна програма.

корисні моделі, які виникли у процесі виконання Договору і на які видані документи виключного права»;

— *об'єкт авторського права* — «використані у комплекті науково-технічної документації наслідки творчої діяльності окремих громадян або їх колективів, створені у результаті виконання Договору, якщо таке право зареєстроване в офіційних державних реєстрах України і на яке отримано відповідне свідоцтво». При передачі науково-технічної продукції, тобто вже матеріального об'єкта, третім особам замовник (виконавець) — на цьому етапі вже дві нібито рівноправні особи — у ліцензійних угодах на передачу прав на промислову власність має підтвердити, що об'єкт ІВ є створеним у службовому порядку. Це положення зумовлює обов'язковість того, що: «виконавець має право здійснювати посередницькі операції з комерційної передачі відповідних результатів науково-технічної продукції за дозволом і під контролем Замовника». Це за умови того, що за одним із пунктів контракту (договору) «Замовник має право на використання переданих йому Виконавцем результатів робіт, а Виконавець може використати отримані результати для власних потреб». Напрошується висновок, що для отримання дозволу «на комерційне використання отриманих результатів» науково-технічної роботи виконавець має виступати у ролі посередника між замовником та покупцем. Природно, що про типові положення з цього приводу не може бути й мови, а для виходу із такого патового стану багато підприємств, організацій створили — кожне на свій страх та ризик, — напівкомерційні структури²⁴⁰.

Цей фактичний стан особливо нестерпний стосовно правових методів використання науково-технічних досягнень, інтелектуальної діяльності в Збройних Силах України. Так, цілком слушно зазначається²⁴¹, що національні закони щодо захисту інтелектуальної власності містять норми, не завжди узгоджені між собою, крім того, одні з них не забезпечують виконання інших. Патентне законодавство України не визначає права держави на інтелектуальну власність, навіть на ту, що створена за кошти державного бюджету, не розглядає питання розподілу прав на об'єкти інтелектуальної власності між замовником, виконавцем робіт та авторами створених об'єктів. І зовсім не зачіпає питання інтелектуальної власності стосовно національ-

ної безпеки. «У результаті такої правової колізії наша держава сьогодні неспроможна повною мірою розпоряджатися результатами науково-дослідних і дослідно-конструкторських робіт, зокрема воєнного, спеціального та подвійного призначення, що фінансуються за рахунок коштів її бюджету»²⁴². Як наслідок, держава не повністю отримує прибутки від профінансованих нею робіт, а то й зазнає прямих збитків. Ілюстрацією до цього є Закон України «Про державне оборонне замовлення», який визначає, що використання результатів науково-дослідних та дослідно-конструкторських робіт, отриманих під час виконання оборонного замовлення, а також розроблення технологій військового та спеціального призначення здійснюється за погодженням з державними замовниками відповідно до законодавства України з питань промислової власності. Розділ «Право на одержання патенту» Закону «Про охорону прав на винаходи і корисні моделі» не розглядає відносин між державним замовником, роботодавцем та автором винаходу у разі створення об'єкта інтелектуальної власності за рахунок коштів державного бюджету. Наслідком відсутності положень прямої дії про розподіл прав на інтелектуальну власність, створену при виконанні робіт за державним замовленням, є вірогідне збільшення вартості продукції, яку придбавають для державних потреб, а також неможливість пільгового стимулювання створення таких об'єктів інтелектуальної власності в суспільно важливих інноваційних процесах та можливий перехід прав на створені за державні кошти об'єкти інтелектуальної власності до іноземних власників з відповідним зниженням конкурентоспроможності вітчизняних виробників.

Використовуючи результати НДДКР, у тому числі надані в інформаційному вигляді, необхідно виходити із реальних можливостей такого використання, а також з інтересів держави та суспільства. При цьому для суспільства (платників податків) не є принципово важливим, яка із сторін отримує більше прав — замовник (держава) чи виконавець (юридична чи фізична особа). Особливо є небажаними двозначності типу спільного володіння документом (звітом, технічною документацією) або патентом як виконавцем, так і замовником, а також необхідність додаткових дозволів або узгоджень²⁴³. На практиці, за наполяганням замовника — державного органу, до договору чи контракту

включають умову, за якою «всі права на отримувані результати НДДКР» належать замовнику. Виконавець втрачає будь-які права та можливості включити, тим більше, планово включити, у господарський обіг ці результати, а замовник такої можливості взагалі не отримує, оскільки будь-який орган державного управління може робити лише те, що зобов'язаний, і не більше. Будь-який відступ від цього принципу породжує численні порушення законодавства, правил бухгалтерського обліку та інших норм. Іншими словами, намагання закріпити всі права на результати НДДКР за замовником призводить до ситуації, коли одна сторона позбавлена прав на використання результатів за своїм статусом, а інша — за умовами договору.

Традиційно ринкові обміни здійснюються лише тоді, коли з них мають користь обидві сторони, що вступають у такий обмін. Але з урахуванням витрат на трансакції або трансакційних витрат, користь, що отримується обома сторонами, має бути більшою від трансакційних витрат, до того ж згадана умова має виконуватися для кожної зі сторін. Виконання цих умов і має забезпечувати ринок²⁴⁴.

Відмінність вітчизняних конфліктів з приводу прав на результати інтелектуальної, передусім науково-технічної, діяльності від західних не зводиться лише до відсутності в Україні механізмів примусового виконання патентних норм та правового нігілізму вітчизняного бізнесу. Навпаки, йдеться про цілком законні, іноді вельми витончені засоби позбавлення зиску окремими особами та групами осіб — держави чи один одного, тобто саме про використання прав і навіть про зловживання правами, а не про пересічне ігнорування чужих прав.

Актуальність проблеми специфікації, тобто встановлення і закріплення прав на інформаційний та матеріальний вид НДДКР і включення їх у цивільний оборот, для сучасної України важко переоцінити, оскільки з різних причин не повністю специфіковано права практично на всі результати науково-дослідної діяльності, що має походження ще з радянських часів. До того ж лише деякі економісти, державні чиновники та керівники великих наукових, науково-виробничих центрів розуміють, що багато проблем комерціалізації технологій породжені саме неповнотою специфікацій прав на них. Передусім це стосується

технологій подвійного призначення. Слід зауважити, що проблема ефективності використання цих технологій у цивільному секторі промисловості виникала й у США, але кожного разу, коли така тенденція спостерігалась, урядом негайно вживались заходи щодо виправлення такого стану²⁴⁵.

З усієї сфери професійної діяльності, пов'язаної із проблемою власності на інформаційні та матеріальні об'єкти, що створюються у процесі інтелектуальної діяльності, для цілей цього дослідження, виділимо трансакції (угоди, але не тільки), спрямовані на введення у господарський та/або комерційний обіг результатів науково-технічної діяльності і закріплені в охоронній формі: а) документації з НДДКР, виконаної за держзамовленням повністю або частково; б) патентів; в) продукції, що підлягає ліцензуванню. Торговельне право щодо цих результатів є вельми широким, таким, що поширюється на всі розділи права і навіть на окремі правові норми, які визначають умови торгівлі та конкуренції на товарних ринках. Власне «ринок прав» на інформаційні та матеріальні результати інтелектуальної діяльності включає: законодавство про інтелектуальну власність, антимонопольне, податкове та інформаційне, що посилено розробляється останнім часом.

Фактично форми інформаційного обігу, передусім ринкові, залежать від наявності (відсутності) та порядку системи оформлення прав на результати інтелектуальної діяльності. Це можна подати як ланцюжок: права (*на ІВ*), від яких залежить *оцінка ІВ*, від яких залежить можливість *комерціалізації результату науково-технічної діяльності* (як прикладних розробок, так і фундаментальних досліджень).

Право фіксується після виконання трьох етапів: реєстрації результату, тобто завершеного дослідження (НДДКР); експертизи — інформаційної та матеріальної складових результату дослідження; видачі, тобто унявлення чи оформлення, охоронного документа та забезпечення заходів щодо його підтримки. Тоді створення інформаційно-аналітичної системи підтримки ринку чи впровадження ринкових форм інформаційного обігу може спиратися на відтворену в системі реєстрації та обліку інформацію (дані, відомості, документація), що використовується у процесі комерціалізації результатів науково-технічної діяльності.

У розрізі трансферу технологій документація являє собою оформлену в установленому порядку та зафіксовану на матеріальному носії інформацію про технології та їх об'єкти (нормативна, науково-технічна, конструкторська документація, звіти про результати патенто-кон'юнктурних, наукових і науково-прикладних досліджень, конструкторських і проектних робіт, державних випробувань об'єктів технологій), наявність якої забезпечує їх використання.

Для НДДКР етап реєстрації, тобто сам факт реєстрації, і є ознакою, що це — науково-дослідна, дослідно-конструкторська розробка. Ніякого іншого охоронного документа, крім довідки про реєстрацію виконаної (завершеної) НДДКР, таке дослідження не отримує. Експертиза результату дослідження фактично здійснюється на стадії здачі-приймання і отримує оформлення у вигляді акта приймання НДДКР за підписами приймальної комісії, яка являє собою виробничу експертну раду. Однак така експертна рада може тільки підтвердити факт відповідності отриманого результату умовам, висунутим у технічному завданні, та рівень виконання робіт, що аж ніяк не є подібним до патентної експертизи, хоча фахівці з приймальної комісії за своїми професійними знаннями можуть мати набагато вищий рівень кваліфікації та досвіду, ніж патентознавці. Цей акт і є нібито охоронним документом, який підтверджує науковий статус (не рівень!) дослідження, але не надає і не визначає ніяких підстав щодо можливості комерційного використання розробки конкретною особою — автором, виконавцем (юридична особа), замовником (орган державного управління). Не в останню чергу така ситуація зумовлює те, що далеко не всі звіти з НДДКР, виконані за кошти держбюджету, потрапляють до державної системи реєстрації, яка в Україні здійснюється УкрІНТЕІ. Зниження рівня вимог до державного контролю обліку НДДКР з відкритої та закритої тематики певною мірою зумовлено недостатньою розробкою цих питань у постановах Кабінету Міністрів України²⁴⁶. Така ситуація призвела до різкого порушення балансу між реальним обсягом НДДКР, що виконуються у країні за рахунок держбюджету, та кількістю інформаційної науково-технічної продукції (звіти про НДДКР), що надходять до державних фондів для охорони та збереження. Тобто має місце неправомірне приховування, хоча й не навмисне, державного

майна, створеного за кошти держбюджету, у формі інтелектуальної власності, яка міститься в інформаційній продукції з НДДКР.

Особливості обліку та організації обігу нематеріальних активів у вітчизняній системі бухгалтерського обліку не дають змоги зробити їх реальними у вартісному та правовому аспектах, правомірно та обґрунтовано вкладати їх у статутні фонди юридичних осіб, захищати від розкрадання чи знищення при приватизації, реорганізації та ліквідації підприємств науково-технічної сфери²⁴⁷.

Нематеріальні активи — це узагальнене поняття, що використовується для визначення активів підприємств, організацій, фірм, які не мають фізичного змісту і характеризуються такими властивостями:

- мають вартісну ознаку та здатність давати прибуток;
- використовуються у фінансово-господарській діяльності понад один рік;
- реалізуються у вигляді прав, що впливають із патентів, свідоцтв, ліцензійних та авторських угод, є результатами інтелектуальної праці²⁴⁸.

Інтелектуальна власність не виникла раптово з нічого на початку 1990-х років, вона, звичайно, існувала і в епоху планового господарства. Річ у тому, що ІВ у фінансово-господарській діяльності практично не використовувалась як нематеріальні активи, як об'єкт ринкових відносин. Особливо це стосується інформаційної складової величезного масиву розробок найрізноманітнішого призначення, який був створений та накопичений за попередній період і тепер настав час ним розпорядитися, але за суттєво інших умов господарювання у державі.

Ще й досі відмітною рисою вітчизняної економіки є традиційний та звичайний пріоритет матеріальної сфери без урахування інформаційної сутності, що відтворює інтелектуальну працю при створенні науково-технічних об'єктів, тоді як у країнах з розвинутою ринковою економікою такої власності — інформаційній, інтелектуальній — надається першочергового значення²⁴⁹.

Тут також необхідне не тільки детальне знання нормативних актів, а й правильне оформлення відповідних юридично значущих документів. Єдиний нормативний акт — Порядок експертної оцінки нематеріальних активів, розроблений Фондом

державного майна України²⁵⁰, передбачає лише експертну оцінку неврахованих матеріальних активів під час приватизації. Запропонована методологія оцінки вартості підприємств, крім того, що стосується головним чином оцінки майна, дещо відрізняється від загальноприйнятих у світі. Спеціалісти висловлюють сумнів щодо використання цієї методики для підприємств, де велику частку їхньої вартості становлять саме права інтелектуальної власності²⁵¹. За власниками таких прав не закріплюється нормативно-правовим актом будь-якого рівня триада правових функцій, якими наділено власника матеріальних об'єктів: володіння, користування і розпорядження²⁵². І це тоді як комплекс прав на об'єкти інтелектуальної власності (нематеріальні активи) багатьох компаній за кордоном оцінюється експертами у десятки мільярдів доларів²⁵³. Слід підкреслити, що кожен тип інтелектуальної власності, визначений, наприклад, у Законі України «Про захист прав на винаходи і корисні моделі»²⁵⁴, має свою специфіку, притаманну його природі, і з правового погляду підлягає регулюванню іншими законами, але економічна властивість прав є однаковою щодо них як до категорії нематеріальних активів.

З погляду на особливості виникнення інформації з науково-технічного доробку країни, її правового захисту включно з правилами перетинання державних кордонів, сучасні способи збереження і надання через електронні засоби обробки і зв'язку та практично не розроблений порядок використання НТІ як результату науково-технічної діяльності, у тому числі у ринкових формах інформаційного обігу, спостерігаються дві основні тенденції функціонального спрямування правового поля щодо інформаційного ресурсу держави: регулятивна та захисна.

Регулятивна функція спрямовується на визначення етапів виникнення, збору, обробки, збереження та надання інформації, що обумовлюється системою угод або домовленостей між власником першоджерел та розпорядником фонду даних чи відомостей певного типу.

Захисна функція забезпечує порядок використання змістовних даних та визначає порядок доступу до масивів інформації, організованих певним чином та за допомогою відповідного інструментарію (у тому числі технічних засобів).

Змістовний інформаційний ресурс, що вводиться до господарського обігу як стратегічний ресурс суспільства, може бути об'єктом власності різних суб'єктів господарювання та розглядатися як продукт переробки у різних інформаційних системах з правовим режимом обробки, що встановлюється власником засобів обробки відповідно до визначеного законодавством правового режиму конкретного виду ЗІР. Тут є дієвими умови власника першоджерел та власника інформаційної системи щодо способу обробки та збереження змістовних даних першоджерела. Нова інформація як продукт обробки, що виникає згідно з конкретним технологічним циклом, що включає засоби обробки та персонал, є власністю власника цих засобів або власністю замовника опрацьованої інформації (за системою угод) або власністю користувача інформаційної системи (за порядком інформаційного забезпечення). При цьому умови, за якими була здійснена передача першоджерела до інформаційної системи, є домінуючими, а тому права власника мають ураховуватися насамперед при оплаті (чи в умовах передачі) нової, опрацьованої в ІС, інформації її замовником.

Таким чином, щоб бути або стати компонентом ЗІР, що використовується суспільством, інформація повинна мати визначений правовий режим на всіх етапах свого виникнення, і це має бути зареєстровано та піддано подальшому обліку відповідно до правових норм, виконання яких має бути підконтрольним державі.

Беручи до уваги властивість інформації як товару перетворювати корисність природного продукту або продукту діяльності людини на комерційну цінність, а сам продукт — на ринковий товар, стає просто необхідним розглядати інформаційний ринок як інституцію, що має на меті полегшення умов інформаційного обміну чи, іншими словами, зниження транзакційних витрат у процесі інформаційного обміну.

Для здійснення таких кроків слід повернутися передусім до вдосконалення закону про НТІ, доповнити його положеннями про формування та використання державних ресурсів НТІ, особливо у частині, що стосується патентоне захищеної інформації, з урахуванням глобалізації інформаційних мереж та електронних баз даних, інноваційної діяльності та захисту інтелектуаль-

ної власності на наукові, науково-технічні та технологічні розробки і науково-технічну продукцію.

Як зазначалося, трансакційні витрати правовласника інформації становлять чималу перешкоду в процесі використання результатів науково-технічної діяльності. Для комерціалізації таких результатів або просто грамотного впровадження у виробництво потрібні окремо виділені посередники як уповноважені організації з обліку нематеріальних активів та довірчого управління ними у частині результатів НДДКР, виконаних за бюджетний рахунок та за кошти інвесторів (звичайно, за побажанням останніх). Узв'язку з цим також важливо забезпечити у єдиній СНІР високоефективну роботу системи обліку та контролю об'єктів інтелектуальної власності (за науково-технічним доробком) державного рівня та визначити центральний український депозитарій НТІ, функції якого в дуже обмеженому, зародковому вигляді в даний час виконує УкрІНТЕІ²⁵⁵.

Можна стверджувати, що сьогодні інституція посередництва виникає повсюдно через труднощі отримання релевантної інформації з питання, що цікавить споживача як такого, з метою створення та/або розвитку виробництва чи започаткування власного бізнесу. Посередницькі структури, що працюють на ринку, є значною мірою спеціалізованими. Якщо спектр їхніх можливостей є навіть досить широким, все одно якомусь певному напрямку, з різних обставин, надається більша перевага. Але оскільки система реєстрації, обліку та видачі охоронних документів за результатами науково-технічної діяльності має фінансову основу державного замовлення, тобто здійснення фінансування з коштів держбюджету, то потрібний і структурний підрозділ на рівні органів центральної виконавчої влади, у віданні якого перебували б зазначені питання з комерційного використання результатів науково-технічної діяльності. Більш того, якщо якась розробка була виконана не за рахунок держбюджету, але застосована чи була впроваджена у державному секторі виробництва або такому, що контролюється державою, це також має бути у полі зору організаційної структури, що пропонується.

Одним із завдань, що постають перед цією структурою, є розширення мережі організацій, які фахово працюють на ринку надання консалтингових або посередницьких послуг з просу-

вання перспективних проектів та їх інвестиційного фінансування, визначення функцій та правового статусу технологічних брокерів наукових центрів, венчурних фондів галузевого та міжгалузевого рівнів. Більш того, це має визначальний характер у зв'язку з ціною дискримінацією у наукоємних галузях, поступовим витісненням патентної охорони результатів інтелектуальної діяльності більш динамічними способами охорони за допомогою авторського права у поєднанні із засекречуванням технологій²⁵⁶. Тенденція зростання ролі секретів виробництва у охороні технологій пов'язана з великою вартістю трансакційних витрат у процесі здійснення права на охорону об'єкта інтелектуальної власності та надто при комерціалізації науково-технічних досягнень. Справді, тільки оформлення відповідних юридичних документів потребує залучення патентних повірених, аудиторів, незалежних оцінювачів, що є тривалим та дорогим процесом²⁵⁷. Також доведення факту порушення патенту, якщо це мало місце, також пов'язане з великими витратами на послуги патентних повірених (можливо, і не вітчизняних), експертів та адвокатів, тобто з великими трансакційними витратами. Фактично патентна охорона технологій стає доступною лише великим фірмам, причому надійність охорони не є забезпеченою й у цьому випадку. Збереження технології у секреті коштує значно дешевше. Більш того, надійність патентної охорони весь час знижується, тоді як надійність охорони секретів виробництва скоріше підвищується, ніж спадає. Витрати специфікації та охорони виключних прав зростають швидше, ніж при охороні тих самих технологій у режимі комерційної таємниці (секретів виробництва). Прямо навпаки все відбувається при використанні тих самих інституцій для охорони кінцевих продуктів. Установити факт порушення патенту в цьому випадку порівняно легко, а засекретити конструкцію майже неможливо. Тому патентна охорона дедалі більше рухається у напрямі охорони кінцевих виробів, тоді як для охорони технологій у їх інформаційному аспекті все більше використовується інституція комерційної таємниці²⁵⁸.

Найактуальнішою проблемою залишається недосконалість патентної охорони винаходів та інших об'єктів промислової власності. Показовою є оцінка стану справ у цьому плані, яку дає академік А.П.ІПпак. Він пише: «Для того, щоб одержати патент

із проведенням експертизи по суті, необхідно чекати чотири — п'ять років, що практично унеможливляє укладання ліцензійних договорів. Це призводить до того, що наукові установи вимушені патентувати розробки в Росії, де можна одержати патент за рік-півтора, а потім вже на підставі російського патенту одержати український». До того ж введення п'ятирічних декларативних патентів без проведення експертизи по суті себе не виправдало. У зв'язку з цим, на думку автора, організація видачі в Україні повноцінних патентів та внесення відповідних змін до чинного законодавства є невідкладним важливим завданням²⁵⁹.

І ще один значний аспект цієї проблеми (про який йшлося на міжнародному симпозиумі у Києві у вересні 2001 року) пов'язаний із правовою незахищеністю українських авторів науково-технічних розробок при їх виході на світовий ринок та патентування за кордоном. У зв'язку з низьким рівнем матеріальної забезпеченості наших учених практично повністю виключається можливість оплатити закордонне патентування. Вчені шукають зацікавлених зарубіжних партнерів, передаючи їм іноді на грабіжницьких умовах частину своїх авторських прав, та поступаються інтересами держави²⁶⁰.

Розглянуті ситуації свідчать про те, що в Україні не вироблені адекватні механізми захисту інтересів держави та збереження коштів платників податків, коли інтелектуальна власність створюється за рахунок бюджетних коштів, зокрема у вигляді інформаційної складової НДДКР.

Ця ситуація поглиблюється відсутністю в Україні законодавчих актів у сфері службових винаходів, а також будь-яких правових актів, що регламентують роботу із заявками на секретні винаходи, які були подані заявниками ще у період існування СРСР. Стосовно реалізації прав на об'єкти промислової власності в Україні діє Положення про порядок оформлення і використання прав на винаходи, корисні моделі і промислові заразки, що становлять державну таємницю, затверджене постановою Верховної Ради України у 1995 році²⁶¹. Однак дія цього положення не поширюється на заявки про секретні винаходи, подані заявниками у радянський період. У даний час налічується до півмільйона діючих охоронних документів — авторських свідоцтв з грифом «Для службового користування», які ніколи

не публікувались у відкритій пресі й тому становлять потенційну загрозу як для російських, так і для іноземних (щодо РФ), у тому числі українських, патентовласників²⁶². Цей масив дістався у спадок Росії — за невідомо ким визначеним правом — від СРСР, у якому існувало чотири види охоронних документів на винаходи: патенти та звичайні авторські свідоцтва на винаходи, описи яких публікувались і були включені до обов'язкового мінімуму патентної документації згідно з Інструкцією до Договору про патентну кооперацію; авторські свідоцтва з грифом «Для службового користування», описи яких закриті для широкої громадськості і повністю недоступні для іноземних громадян, що є порушенням Паризької конвенції; секретні авторські винаходи, описи яких взагалі не публікувались²⁶³.

Авторські свідоцтва з грифом «Для службового користування» є унікальними. Кожне з них відповідно до Постанови Верховної Ради РФ «Про введення в дію Патентного закону Російської Федерації» може бути перетворене на патент РФ. Тобто у будь-який момент протягом 20 років з дати подання заявки можлива зовсім несподівана для третіх осіб поява патенту, що зачіпатиме їхні права. Цій проблемі не приділяється ніякої уваги, але з часом вона заплутується все більше, оскільки численні юридичні особи, на ім'я яких видані такі свідоцтва, вже не існують або є вже іншими юридичними особами, часто з іншою — недержавною — формою власності. Ця проблема може бути вирішеною тільки в результаті активних дій державних органів управління у взаємозв'язку з аналогічними органами країн СНД. Очевидно, що підприємствам-власникам ІВ взагалі, а у галузі документації з обмеженим доступом зокрема доведеться виконати досить трудомістку підготовчу роботу з відповідними витратами, щоб стати активним учасником ринку інтелектуальної власності та ринкових форм інформаційного обігу.

Як зазначалося, нематеріальні активи — це те, що забезпечує підприємству прибуток або інший додатковий ефект порівняно з аналогічними суб'єктами господарювання. Ця інформація у ряді випадків має конфіденційний характер і тому належить до джерел обмеженого поширення. Загальноприйнята правова класифікація конфіденційної інформації на сьогодні відсутня, що створює певні труднощі при реалізації як внутрішніх, так і зовнішніх ринкових відносин. Так, ряд міжна-

родних угод, зокрема Паризька конвенція з охорони промислової власності, передбачає, що захист комерційної таємниці як складова антимонопольно! діяльності включається до складу об'єктів промислової і, як наслідок, інтелектуальної власності. Але в Україні законодавство з ІВ та антимонопольне законодавство є розділеними. Також потребує вирішення питання щодо суб'єктів права на долучення відомостей до комерційної таємниці. Не можна погодитися з тим, що за Законом України «Про підприємства в Україні» суб'єктами права щодо комерційної таємниці визнаються лише підприємства. Потрібно чіткіше визначити поняття комерційної та службової таємниць та розмежувати їх. Маємо також враховувати, що у чинному законодавстві не міститься норм, які регламентували б порядок оцінки документованої інформації та інформаційних ресурсів та зарахування їх на баланс. Для реальної задіяності таких законодавчих норм є необхідним внесення значних змін не тільки у закони про НТІ та ІВ, а й до чинного цивільного та фінансового законодавства, що у свою чергу передбачає їхній глибокий аналіз.

Небезпека тиражування (копіювання) інформації та її переміщення поглиблюється тим, що вона, як правило, відчувається від власника, тобто зберігається та підлягає обробці у сфері доступності великої кількості суб'єктів, що не є суб'єктами права власності на неї. Це, наприклад, автоматизовані ІС, у тому числі територіально розподілені державні і корпоративні мережі. Тобто до інформації, або узагальнено до ЗІР, за винятком суб'єкта права власності на цю інформацію, можуть мати доступ й інші особи як законно, санкціоновано (наприклад, за угодою чи за умовами праці), так і незаконно, несанкціоновано. Виникає складна система взаємовідносин між цими суб'єктами права власності та необхідних ланок, що забезпечують доступ до інформації. Закон має врегулювати відносини суб'єктів та об'єктів права власності на інформацію (ЗІР) з метою захисту прав як власників, так і споживачів від розголошення, витоку, несанкціонованого ознайомлення, її обробки, зокрема копіювання, модифікації або знищення, або, за прийнятою термінологією, — від несанкціонованого доступу та порушення її цілісності.

Головною метою державного регулювання діяльності у сфері трансферу технологій має бути забезпечення сталого зростання

національного промислового і науково-технічного потенціалу, його ефективне використання для вирішення завдань соціально-економічного розвитку держави та підвищення технологічності виробництва вітчизняної продукції з урахуванням світового досвіду, можливих соціально-економічних, технологічних і екологічних наслідків від застосування технологій (їх об'єктів), сприяння розвитку виробництва, в якому використовуються новітні вітчизняні технології. Під технологією, у даному контексті, автор розуміє результати інтелектуальної діяльності, сукупність систематизованих наукових знань, відпрацьованих технічних, організаційних та інших рішень у вигляді документації про застосування відповідного технологічного процесу, обладнання, що використовуються для виробництва продукції, послуги, які надаються при здійсненні зазначеного виробництва, а також про перелік, строки, порядок та послідовність виконання технологічних операцій процесу виробництва, реалізації та зберігання продукції. При цьому під технологіями подвійного використання слід розуміти такі технології, які, крім створення продукції для задоволення цивільних потреб, можуть бути використані для розроблення, виробництва або використання озброєння, військової або спеціальної техніки.

Управління може здійснюватися при виконанні кількох умов, зокрема: наявності спостереження об'єкта управління; наявності його керованості; наявності мети управління; наявності свободи вибору рішень суб'єктом управління; наявності критерію (критеріїв) управління; наявності ресурсів (матеріальних, фінансових, інтелектуальних, інформаційних тощо). У ході наших подальших роздумів ми ще повернемося до порядку визначення функцій і структури державних органів, який би не суперечив науці управління: «мета —> функції —> структура». Тут же зауважимо, що функція будь-якого соціального інституту є способом його адаптації в суспільстві, встановленням відносин між ним і визначеною потребою суспільства. Саме ці відносини мають визначатися і регулюватися законодавством. Тому, визначивши головну мету державного регулювання діяльності у сфері трансферу технологій і зберігаючи послідовність в даному конкретному випадку, розглянемо функції, які має виконувати держава в цій сфері. Для цього спробуємо визначити такі основні функції (табл. 2) і потім зробимо їх «прив'язку» до суб'єктів

трансферу технологій. Суб'єктами трансферу технологій можуть розглядатися такі, як: уповноважений державний орган — центральний орган виконавчої влади з питань наукової, науково-технічної, інноваційної діяльності та інтелектуальної власності (1), а також інші центральні та місцеві органи виконавчої влади, органи місцевого самоврядування, які беруть участь у закупівлі, переданні і/або використанні об'єктів технологій (2); Національна та галузеві академії наук, наукові установи, що створюють вітчизняні об'єкти технологій та яким належать майнові права на об'єкти права інтелектуальної власності, які є об'єктами технологій (3); науково-виробничі об'єднання, підприємства, установи і організації незалежно від форми власності, які використовують технології (їх об'єкти), в тому числі майнові права на об'єкти права інтелектуальної власності, які є об'єктами технологій (4); фізичні особи, які беруть безпосередню участь у створенні, трансфері та впровадженні технологій, надають інформаційні, фінансові та інші послуги на всіх стадіях просування технологій (їх об'єктів) на ринок (5); постачальники об'єктів технологій та сировини, що використовуються під час застосування технологій (6); юридичні та фізичні особи, що надають технічні послуги, пов'язані із застосуванням технологій (7). Обмежимося розглядом функцій перших трьох суб'єктів трансферу технологій (табл. 2).

У контексті питання трансферу технологій, що розглядаються, потребують пояснення визначення таких термінів, як «патентна чистота» і «патентно-кон'юнктурні» дослідження.

Зазначимо, що під патентною чистотою слід розуміти власність технологій (їх об'єктів) бути вільно використаними в певній державі без небезпеки порушення діючих на її території охоронних документів (патентів) на об'єкти права інтелектуальної власності, які належать третім особам, визначена відповідно до діючих охоронних документів (патентів) на ці об'єкти та нормативно-правових актів держави (групи держав), де планується використання зазначених технологій (їх об'єктів), а також відповідно до конкретного періоду часу, обумовленого строком дії охоронних документів (патентів) на об'єкти технологій на території такої держави (групи держав).

Патентно-кон'юнктурні дослідження — це системний науковий аналіз властивостей технологій (їх об'єктів), що впливають

Таблиця 2
Основні функції і завдання суб'єктів трансферу технологій

Основні функції та завдання		Суб'єкти трансферу технологій			Примітки
1	2	1	2	3	
1	2	3	4	5	6
1	Забезпечення реалізації державної політики у сфері трансферу технологій	*			
2	Координація дій та здійснення контролю, що пов'язані з набуттям та передачею прав на технології (їх об'єкти), для сприяння розвитку вітчизняних технологій, виробництву вітчизняної конкурентоспроможної продукції	*			
3	Створення і ведення міжгалузевого банку даних про вітчизняні та іноземні технології і організація поширення інформації про технології, які можуть бути використані для технологічного оновлення вітчизняних підприємств.	*			
4	Формування і ведення державного реєстру технологій, визначає потребу у патентуванні, передачі і/або придбанні прав на об'єкти технологій в Україні та за її межами		—	—	—
5	Узгодження з реальними потребами виробників продукції програми наукових досліджень, проектних та конструкторських робіт, пов'язаних із створенням об'єктів технологій, враховуючи при цьому суспільні та державні потреби у такій продукції		—	—	—
6	Здійснення конкурсного відбору пропозицій з розроблення нових технологій та їх об'єктів для модернізації існуючих виробництв та забезпечення їх фінансової підтримки		—	—	—
7	Подання Кабінету Міністрів України пропозицій до проектів державних програм технологічного оновлення галузей промисловості стосовно набуття або передачі прав на технології (їх об'єкти)	*			
8	Стимулювання створення та використання високих технологій	*			

1	2	3	4	5	6
9	Державна експертиза та державна реєстрація договорів з трансферу технологій, ведення державного реєстру відповідних договорів	*			
10	Здійснення перевірки дотримання прав на технології (їх об'єкти)	л			
11	Здійснення заходів щодо недопущення недобросовісної конкуренції, контрафакції і несанкціонованого розповсюдження технологій та конфіденційної інформації про них, поширення технологій подвійного використання без дозволу власника майнових прав на них	*			
12	Контроль за додержанням законодавства про державну таємницю в процесі проведення операцій з трансферу технологій	*	*		
13	Забезпечення підбору потенційних контрагентів для трансферу технологій	л			
14	Підтримка розвитку інфраструктури у сфері трансферу технологій і стимулювання залучення інвестицій	*	—	—	—
15	Надання консультаційно-методичної допомоги з питань укладення договорів про трансфер технологій, подання заявок на одержання охоронних документів на об'єкти технологій в Україні та за її межами	*			
16	Здійснює в системі вищої освіти програму підготовки фахівців з питань інтелектуальної власності, трансферу технологій та управління інноваційною діяльністю	*	—	—	—
17	Координація галузевої підготовки та перепідготовки фахівців з питань інтелектуальної власності, трансферу технологій та управління інноваційною діяльністю	*	—	—	—
18	Запобігання, виявлення та припинення порушень у галузі інтелектуальної власності та трансферу технологій уповноважений орган у взаємодії з органами МВС України, ДПА України, СБ України та засобами масової інформації	*			

1	2	3	4	5	6
19	Проведення патентно-кон'юнктурних досліджень та досліджень на патентну чистоту		—	—	—
20	Моніторинг науково-технологічної сфери і ринку технологій у країні та за кордоном		*		
21	Формування баз даних про технології (їх об'єкти), майнові права на які належать відповідному центральному органу виконавчої влади або академії наук, забезпечують доступ до них осіб, заінтересованих у використанні певних технологій (їх об'єктів)	—			—
22	Формування галузевих реєстрів технологій (їх об'єктів) і подання клопотання на включення певних технологій (їх об'єктів) до Державного реєстру технологій	—			—
23	Розроблення галузевих комплексних програм технологічного оновлення підприємств та забезпечення їх виконання		*	*	—
24	Сприяння створенню імпортозамінних об'єктів технологій		*	*	
25	Сприяють залученню інвестицій до виконання програм технологічного оновлення вітчизняних підприємств	—	—		—
26	Подання уповноваженому органу пропозицій щодо найефективніших шляхів використання чи трансферу технологій (їх об'єктів), насамперед вітчизняних	—			—
27	Забезпечення захисту прав на об'єкти права інтелектуальної власності, які є об'єктами технологій і подання уповноваженому органу клопотання про необхідність патентування та ліцензування прав на певні об'єкти технологій за межами України. Участь у підготовці договорів про трансфер технологій	—			—
28	Забезпечення контролю за додержанням вимог міжнародних договорів України щодо запобігання техногенному ризику, поширенню потенційно небезпечних технологій та щодо екологічної безпеки технологій		*		

1	2	3	4	5	6
29	Подання до уповноваженого органу звітів про патентно-кон'юнктурні, наукові дослідження, конструкторські, проектні, випробувальні роботи, пов'язані із створенням і використанням технологій (їх об'єктів), патентуванням і ліцензуванням прав на них та про виплату винагороди їх авторам		*	*	
30	Здійснення контролю за переданням майнових прав на технології (їх об'єкти) науково-виробничим об'єднанням та підприємствам, до сфери діяльності яких належить використання цих технологій, - а також за виплатою ними винагороди авторам об'єктів технологій відповідно до укладеного з ними договору		*	*	
31	Контроль за веденням обліку об'єктів технологій у складі майна науково-виробничих об'єднань, підприємств, установ і організацій, яким передані права на їх використання, у тому числі нематеріальних активів, які є такими об'єктами	—	*	*	—
32	Розробка проектів регіональних програм технологічного переоснащення підприємств, що належать до комунальної власності відповідних територіальних громад, та подання їх на затвердження Верховній Раді Автономної Республіки Крим, обласним і районним радам		*		
33	Створення регіональних баз даних про технології (їх об'єкти), забезпечення поширення інформації про технологічні потреби регіону		*		
34	Сприяння розробці та використанню відповідних технологій		„	»	
35	Участь у міжнародному технологічному співробітництві, сприяння залученню іноземних інвестицій для технологічного переоснащення підприємств регіону		*	*	
36	Фінансування досліджень та розробок з розв'язання проблем технологічного переоснащення підприємств регіону в межах передбачених коштів відповідного бюджету	—	*	—	—

з їх правової охорони, стану ринків технологій (їх об'єктів) та продукції, а також патентної та ліцензійної ситуації, що склалася щодо них, характеру виробництва продукції, який здійснюється на основі патентної, науково-технічної, кон'юнктурно-економічної та іншої інформації протягом життєвого циклу технологій (їх об'єктів).

Проведення державної експертизи технологій та патентно-кон'юнктурних досліджень є функцією установ і організацій державної системи науково-технічної та патентної інформації.

Самого переліку функцій, пов'язаних з організацією трансферу технологій, достатньо для усвідомлення того, що для забезпечення їх виконання у складі уповноваженого органу, інших центральних органів виконавчої влади, Національної та галузевих академій наук, а також на провідних підприємствах, установах і організаціях мають створюватися структурні підрозділи з питань інтелектуальної власності та трансферу технологій.

Важлива роль у питаннях інтелектуальної власності та трансферу технологій належить Раді міністрів Автономної Республіки Крим, місцевим органам виконавчої влади та виконавчим органам сільських, селищних, міських рад.

Суб'єкти трансферу технологій здійснюють взаємодію між собою шляхом: проведення консультацій з основних проблем науково-технологічної політики стосовно застосування технологій (їх об'єктів); обміну досвідом та інформацією щодо науково-технологічних досягнень; виробництва та кооперації поставок об'єктів технологій в рамках договорів про їх трансфер. Тому надзвичайно важливим питанням в умовах ринку технологій є інформаційне забезпечення трансферу технологій. Слід законодавчо закріпити, що уповноважений орган, центральні органи виконавчої влади, Національна та галузеві академії наук у межах своїх повноважень забезпечують інформаційно-консультаційне супроводження трансферу технологій через установи та організації державної системи науково-технічної та патентної інформації шляхом збирання, ведення обліку, архівного зберігання, розповсюдження наукової, конструкторської та проектно-документації, науково-технічної, кон'юнктурно-економічної та патентної інформації, пов'язаної з технологіями (їх об'єктами).

Особлива роль в інформаційному забезпеченні трансферу технологій належить установам і організаціям державної системи науково-технічної та патентної інформації, які забезпечують: формування державної системи науково-технічної, кон'юнктурно-економічної та патентної інформації з урахуванням всіх доступних джерел інформації про об'єкти технологій та створення її регіональних відділень; підготовку за дорученням уповноваженого органу або на замовлення інших центральних органів виконавчої влади, Національної чи галузевих академій наук, заінтересованих підприємств, установ і організацій інформаційно-аналітичних довідок про технології (їх об'єкти) та про трансфер технологій; формування галузевих і регіональних автоматизованих баз даних про вітчизняні та іноземні технології (їх об'єкти), зокрема про патентно-кон'юнктурні, наукові дослідження, конструкторські, проектні та випробувальні роботи, пов'язані зі створенням і використанням зазначених об'єктів, інтеграцію цих баз даних з міжнародними інформаційними мережами з питань трансферу технологій; проведення рекламно-інформаційних заходів, семінарів, конференцій, «круглих столів», виставок, громадського обговорення інформації про технології та їх об'єкти з метою поширення цієї інформації в регіонах; ознайомлення заінтересованих осіб з реферативною патентною інформацією про технології та їх об'єкти на безоплатній основі, надання їм, у встановленому уповноваженим органом порядку, переліку наявних в Україні та за її межами технологій (їх об'єктів), науково-технічної, кон'юнктурно-економічної і патентної інформації про технології (їх об'єкти), якщо майнові права (або частка майнових прав) на них належать державі.

Установи і організації державної системи науково-технічної та патентної інформації для проведення державної експертизи технологій та патентно-кон'юнктурних досліджень мають забезпечити: пошук, систематизацію та аналіз науково-технічної, кон'юнктурно-економічної та патентної інформації про вітчизняні та іноземні технології (їх об'єкти); підготовку аналітичних довідок про вітчизняні та іноземні технології та їх об'єкти.

Слід особливо підкреслити важливість безумовного виконання вимог законодавства України про державну таємницю у всій системі суб'єктів і процедур трансферу технологій.

Важливими формами державного регулювання діяльності у сфері трансферу технологій мають розглядатися такі, як державна експертиза технологій (їх об'єктів), патентно-кон'юнктурні дослідження у сфері трансферу технологій, державна реєстрація договору про трансфер технологій. Усі зазначені процедури мають виконуватися уповноваженим органом у порядку, затвердженому Кабінетом Міністрів України.

Державна експертиза технологій та їх об'єктів, що пропонується для трансферу, передусе державній реєстрації договорів про трансфер технологій і здійснюється уповноваженим органом з метою визначення економічної доцільності та корисності для держави і суспільства впровадження технологій та їх об'єктів, враховуючи можливі екологічні і соціально-економічні наслідки їх застосування. У процесі проведення державної експертизи технологій мають бути обов'язково визначені: технічний рівень і новизна технологій та їх об'єктів; фактична ціна технологій та їх об'єктів; конкурентоспроможність технологій та продукції, яка буде виготовлена із застосуванням цих технологій; патентна чистота об'єктів технологій; переважні умови трансферу технологій; відповідність технологій та їх об'єктів нормам техногенної та екологічної безпеки, технічного регулювання, міжнародним та національним стандартам.

Особа, яка здійснює трансфер технологій за межі України, для проведення державної експертизи технологій та їх об'єктів, зобов'язана подати висновок центрального органу виконавчої влади у сфері державного експортного контролю про відсутність у складі технологій інформації, яка становить державну таємницю, технологій подвійного використання або таких, що належать до сфери національної безпеки і оборони.

Державна експертиза технологій та їх об'єктів, які передбачається ввозити на територію України, має встановити їх відповідність одній з таких вимог: забезпечення підвищення технологічності виробництва продукції, зниження його витратності, енерго- та матеріалоемності; спрямованість на виробництво нової продукції або на вдосконалення якості існуючої; забезпечення використання місцевих матеріальних та людських ресурсів. Вона здійснюється на підставі економічного обґрунтування можливості їх використання на території України або передачі май-

нових прав на них за її межі, звіту про патентно-кон'юнктурні дослідження та патентного формуляра.

Патентно-кон'юнктурні дослідження проводяться при розробленні науково-технічних прогнозів розвитку технологій та їх об'єктів, при їх створенні, визначенні доцільності набуття чи передання прав на них, при підготовці до виробництва з їх застосуванням нової продукції і мають здійснюватися відповідно до державних стандартів і затверджених уповноваженим органом методик.

Патентно-кон'юнктурні дослідження включають: систематизацію відібраної для аналізу патентної, кон'юнктурно-економічної, науково-технічної та іншої інформації про об'єкти технологій; дослідження технічного рівня і тенденцій розвитку технологій та їх об'єктів, а також тенденцій і перспектив розвитку ринку технологій; визначення патентоспроможності і патентної чистоти технологій та їх об'єктів; аналіз динаміки патентування і ліцензування прав на аналогічні об'єкти технологій; визначення фактичного розміру витрат на створення і трансфер технологій та їх об'єктів; аналіз впливу факторів, що визначають кон'юнктуру ринку технологій і продукції, на доцільність застосування певних технологій та виробництво з їх застосуванням продукції; визначення ємності ринку технологій та продукції на підставі суспільних і державних потреб у конкретній технології, її об'єктах, продукції з метою сегментації споживчого ринку технологій та продукції; розроблення заходів щодо запобігання невиправданим витратам, пов'язаним з виробництвом неліквідної продукції; розроблення заходів щодо недопущення несанкціонованого використання об'єктів технологій, контрафакції, недобросовісної конкуренції та перенасичення ринку продукцією; визначення фактичної ціни технологій та їх об'єктів, динаміки зміни цін аналогічних об'єктів і послуг, пов'язаних з їх виробництвом та реалізацією, а також структури цих цін.

Визначення фактичної ціни технологій та їх об'єктів здійснюється шляхом порівняння їх ціни, визначеної виходячи із суми фактичних витрат на створення і заміну об'єктів технологій, із ринковими цінами альтернативних об'єктів технологій, наявних у постачальників, що можуть задовольнити особу, якій передаються зазначена технологія та її об'єкти, за комплексом показників (функціональні властивості, задовільна вартість, три-

валі строки служби, унікальність) та остаточним узгодженням ціни, яка влаштовує сторони договору про трансфер технологій.

Критеріями для визначення фактичної ціни технологій, та їх об'єктів можуть бути такі: витрати на створення і заміну технологій та їх об'єктів з урахуванням їх матеріального та морального зносу; відпускна ціна та балансова вартість технологій та їх об'єктів; ціна аналогічних об'єктів на ринку технологій; сума можливих прибутків від застосування технологій та їх об'єктів.

Зазначимо, що виконання патентно-кон'юнктурних досліджень при визначенні доцільності укладення договору про трансфер технологій передбачає: визначення можливості комерційної реалізації технологій, їх об'єктів та продукції, виготовленої з їх застосуванням, виходячи з кон'юнктури споживчого ринку технологій та продукції, його сегментації та наповненості аналогічними технологіями, їх об'єктами і продукцією, а також державних і суспільних потреб у них; забезпечення рентабельності та технологічності виробництва продукції із застосуванням відповідної технології; встановлення економічних переваг над можливими конкурентами у разі застосування технологій та їх об'єктів для виробництва продукції, а також у разі реалізації цієї продукції. Координацію і проведення патентно-кон'юнктурних досліджень за участю розробників відповідних технологій та їх об'єктів мають здійснювати уповноважений орган, а також центральні органи виконавчої влади, Національна та галузеві академії наук у межах своїх повноважень.

Державна реєстрація договорів про трансфер технологій має здійснюватися у порядку, визначеному Кабінетом Міністрів України, уповноваженим органом, який за результатами державної експертизи технологій (їх об'єктів) приймає рішення про занесення договорів про їх трансфер до державного реєстру. Разом з договором про трансфер технологій на державну реєстрацію мають передаватися висновки державної експертизи та інформація про технологи (їх об'єкти) та охоронні документи на них.

Державна реєстрація договору про трансфер технологій, зокрема, підтверджує: передачу майнових прав на технології (їх об'єкти) певним особам відповідно до законодавства та міжнародних договорів України; недопущення несанкціонованого вико-

ристання об'єктів технологій; схвалення суми ліцензійних платежів за використання технологій (їх об'єктів), а також суми платежів, пов'язаних з поставкою технологічного обладнання та інших об'єктів технологій, визначених договором про трансфер технологій; використання майнових прав на об'єкти права інтелектуальної власності, які є об'єктами технологій, визначених охоронними документами на них, або фактичне використання певного знака для товарів і послуг.

Завершуючи розгляд питань державного регулювання діяльності у сфері трансферу технологій, зазначимо, що ми залишили за рамками нашого розгляду такі аспекти трансферу технологій, як умови укладення договорів про трансфер технологій, види договорів про трансфер технологій, фінансово-економічне забезпечення діяльності у сфері трансферу технологій, зокрема: встановлення винагороди авторам технологій та особам, які здійснюють трансфер технологій; використання коштів, одержаних у результаті трансферу технологій, створених або придбаних за рахунок коштів Державного бюджету України; особливості кредитування трансферу технологій; особливості оподаткування операцій, пов'язаних з трансфером технологій, які потребують законодавчого визначення.

Слід також зазначити, що уповноважений орган разом з центральним органом виконавчої влади, до сфери управління якого належить підприємство, де застосовуватиметься певна технологія, мають передавати цьому підприємству на умовах та в порядку, визначеному Кабінетом Міністрів України, майнові права на технології та їх об'єкти, які є державною власністю. Якщо об'єкти технологій частково створено за рахунок власних коштів підприємств, установ і організацій, а частково — за рахунок коштів Державного бюджету України, майнові права на ці об'єкти мають розподілятися на підставі договору про їх створення пропорційно частці коштів, вкладених у розробку таких об'єктів, та використовуються за умовами договору про їх трансфер.

Міжнародне співробітництво у сфері трансферу технологій означає: укладення двосторонніх і багатосторонніх міжнародних договорів про науково-технічне і технологічне співробітництво; ініціювання залучення інвестицій у науково-технічний

комплекс України; сприяння впровадженню в Україні міжнародних стандартів, зокрема стандартів системи управління якістю; забезпечення участі вітчизняних підприємств, установ і організацій у міжнародних виставках та ярмарках високотехнологічної продукції і технологій; участь у розвитку вітчизняних сегментів міжнародних інформаційних і комунікаційних систем з питань інтелектуальної власності та трансферу технологій.

Уся система трансферу технологій у державі має працювати виключно з позицій довготермінових національних інтересів, враховуючи особливості трансферу технологій підприємствам України. Саме тому необхідно введення законодавчих обмежень щодо укладення договорів про трансфер технологій, які передбачають: ввезення в Україну технологій, які не відповідають вимогам державних програм технологічного оновлення галузей промисловості та можуть завдати шкоди державі, перешкоджають придбанню аналогічних вітчизняних технологій; здійснення виплат, неадекватних фактичній ціні технології та її об'єктів; встановлення зобов'язань щодо придбання в особи, яка передає технологію (її об'єкти), сировини, напівфабрикатів, обладнання та його комплектуючих, що не застосовуються під час виробництва продукції; встановлення зобов'язань щодо переважного продажу продукції, виготовленої із застосуванням технології, покупцям, визначеним особою, яка передає цю технологію, та використання визначеного нею персоналу; право особи, яка передає технологію, визначати ціну продажу або реекспорту продукції, виготовленої із застосуванням технології; встановлення необґрунтованих обмежень обсягу виробництва продукції; встановлення обмежень, які суперечать законодавству, стосовно використання майнових прав на об'єкти технологій; заборону використання аналогічних або більш досконалих об'єктів технологій; заборону або обмеження експорту продукції, виготовленої із застосуванням технології; встановлення зобов'язань щодо використання запатентованого об'єкта інтелектуальної власності, який не використовується в процесі застосування технології; встановлення зобов'язань щодо сплати винагороди власнику свідоцтва на знак для товарів і послуг, який не використовується для маркування продукції, виготовленої із застосуванням технологій та їх об'єктів.

2.3.3. Методика і практика віднесення інформації до категорії з обмеженим доступом

Віднесення інформації до категорії з обмеженим доступом є важливою складовою теорії і практики захисту інформації. Встановлення обмежень доступу — це визначення відповідно до правових норм ступенів секретності (конфіденційності) певної категорії інформації, які характеризують її важливість, порядок доступу до неї та рівень її охорони. Тобто ступінь секретності (конфіденційності) є ступенем обмеження доступу, що диктує всім суб'єктам порядок поведінки з відповідною інформацією.

Віднесення відомостей до інформації з обмеженим доступом — це практична реалізація об'єктивного закону захисту інформації, а саме: примусового відчуження і усупільнення інформації в інтересах суспільної необхідності. У демократичних країнах він всюди реалізується правовими нормами.

В Україні примусове відчуження об'єктів приватної власності може бути застосовано з мотивів суспільної необхідності, на підставі і в порядку, встановлених законом. Такі правові норми містить Конституція України²⁶⁴, Закон України «Про власність»²⁶⁵.

В умовах демократичного суспільства обмеження права власності на інформацію або припинення цього права здійснюється, як правило, на договірних засадах, тобто шляхом укладання відповідного договору між державою і власником відповідної інформації. Стосовно державної таємниці примусове відчуження інформації або її матеріальних носіїв може бути застосоване, як це передбачено законом, лише в інтересах національної безпеки України: «Якщо власник секретної інформації або її матеріальних носіїв відмовляється від укладення договору чи порушує його, за рішенням суду ця інформація або її матеріальні носії можуть бути вилучені у власність держави за умови попереднього і повного відшкодування власникові їх вартості»²⁶⁶.

Безумовно, високий рівень захисту державної таємниці є важливою передумовою формування загальної системи захисту інформації з обмеженим доступом. Участь держави у формуванні системи захисту державної таємниці зумовила те, що віднесення відомостей до цієї категорії та їх засекречування є

всебічно обґрунтованим в методологічному, правовому і організаційному планах як в Україні, так і в інших країнах.

В ній певні особливості має віднесення до державної таємниці та засекречування об'єктів промислової власності, що впливають із вимог Положення про порядок оформлення і використання прав на винаходи, корисні моделі і промислові зразки, що становлять державну таємницю, затвердженого постановою Верховної Ради України у січні 1995 року²⁶⁷.

Цей нормативно-правовий документ розглядає два аспекти вирішення цих питань щодо об'єктів промислової власності, а саме:

— перший, за умов, за яких об'єкт промислової власності створено з використанням інформації, зареєстрованої у Зводі відомостей, що становлять державну таємницю;

— другий, якщо об'єкт промислової власності створено з використанням інформації, яка відповідно до ст.8 Закону України «Про державну таємницю» може бути віднесена до державної таємниці.

В обох наведених випадках автори об'єктів промислової власності мають поводитися з матеріалами на ці об'єкти як з такими, що містять державну таємницю. Заявки на винаходи, корисні моделі і промислові зразки з пропозиціями про віднесення їх до державної таємниці надсилаються до державного патентного відомства.

Державний експерт з питань таємниць на підставі подання державного патентного відомства приймає рішення про віднесення об'єкта промислової власності до державної таємниці, яке реєструється спеціально уповноваженим державним органом з питань охорони державної таємниці.

Винахід, корисна модель, промисловий зразок вважаються секретними об'єктами промислової власності й підлягають засекречуванню з наданням відповідних реквізитів, передбачених ст. 15 Закону України «Про державну таємницю», за умов, що проведена державним патентним відомством експертиза по суті у випадках:

— якщо об'єкт промислової власності створено з використанням відомостей, зареєстрованих у Зводі відомостей, що становлять державну таємницю, з моменту прийняття рішення державним експертом з питань таємниць про віднесення об'єкта

промислової власності до державної таємниці та реєстрації цього рішення спеціально уповноваженим органом з питань охорони державної таємниці;

— якщо об'єкт промислової власності створено з використанням відомостей, що можуть бути віднесені до державної таємниці відповідно до ст. 8 Закону України «Про державну таємницю» — з моменту опублікування відповідних доповнень до Зводу відомостей, що становлять державну таємницю.

Строк дії документа, що засвідчує право авторства на створений об'єкт промислової власності, віднесений до державної таємниці, встановлюється строком засекречування об'єкта промислової власності, однак не більше строку дії патенту на відповідний об'єкт промислової власності, який встановлюється законодавством України з питань охорони промислової власності.

У процесі міжнародного співробітництва інформація, що містить державну таємницю, одержана від інших держав, належить до державної таємниці та засекречується відповідно до вимог національного законодавства. Закон України «Про державну таємницю» цей порядок регламентує таким чином: «Передані Україні відомості, що становлять державну таємницю іноземної держави чи міжнародної організації, охороняються в порядку, передбаченому цим Законом. У разі, якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, встановлені інші, ніж передбачені цим Законом, правила охорони таємниці іноземної держави чи міжнародної організації, то застосовуються правила міжнародного договору України»²⁶⁸. А це передбачає у випадках, якщо національні законодавства сторін містять різні вимоги до порядку обмеження доступу до інформації, що передається (отримується) сторонами, розробку взаємно узгоджених критеріїв і правил вирішення цих питань, які викладаються у вигляді зобов'язань сторін у відповідній угоді (договорі). Наведені вимоги є обов'язковими й у процесі міжнародного наукового і науково-технічного співробітництва з використанням інформації, що становить державну таємницю, та її матеріальних носіїв.

Проте українська система в нових умовах господарювання потребує вдосконалення. Чинні Методичні рекомендації²⁶⁹ не враховують таких факторів, як вигода і перевага відкритого використання відомостей, що підлягають віднесенню до дер-

жавної таємниці; витрат на захист таких відомостей порівняно зі збитками, що можуть бути завдані, у разі їх розголошення.

У США порядок і правила віднесення відомостей до державної таємниці та критерії визначення ступеня їх секретності встановлені директивою Президента США²⁷⁰. У Російській Федерації такі правила і критерії затверджені урядом²⁷¹. В Україні повноваження щодо встановлення критеріїв визначення ступеня секретності інформації Законом України «Про державну таємницю» (редакція 1994 року) були надані колишньому Держкомсекретів України. Цим законом у редакції 1999 року повноваження щодо встановлення критеріїв визначення ступеня секретності надані Службі безпеки України²⁷².

Отже, підстави для віднесення відомостей до державної таємниці та критерії визначення ступенів їх секретності доцільно встановити на рівні не Методичних рекомендацій, а відповідних правил, затверджених Кабінетом Міністрів України. Такі правила будуть обов'язковими для виконання інститутом державних експертів з питань таємниць та державними органами, які розробляють розгорнуті переліки відомостей, що становлять державну таємницю. Окрім того, доцільно, щоб ці правила враховували не тільки сукупну шкоду у разі розголошення відповідних відомостей, а й фактори, пов'язані з перевагою їх відкритого використання, а також витрати на захист таких відомостей.

Необхідність всебічного обґрунтування економічної доцільності віднесення відомостей до державної таємниці зумовлена рядом чинників.

Чинним законодавством встановлено, що фінансування витрат на здійснення діяльності, пов'язаної з державною таємницею, в бюджетних установах і організаціях здійснюється за рахунок Державного бюджету України, бюджету Автономної Республіки Крим та місцевих бюджетів. Кошти на зазначені витрати передбачаються у відповідних бюджетах окремим рядком. Ці витрати інших установ і організацій, а також підприємств відносяться до валових витрат виробника продукції, виготовлення якої пов'язане з державною таємницею.

Витрати на здійснення заходів щодо віднесення інформації до державної таємниці, засекречування, розсекречування та охорони матеріальних носіїв такої інформації, її криптографіч-

ного та технічного захисту, інші витрати, пов'язані з державною таємницею, на недержавних підприємствах, в установах, організаціях фінансуються на підставі договору з замовником робіт, пов'язаних з державною таємницею²⁷³.

Чинне законодавство також передбачає надання відповідної компенсації громадянам за роботу в умовах режимних обмежень²⁷⁴.

Отже, діяльність, пов'язана з державною таємницею, має чітко виражені економічні, вартісні показники у багатьох сферах.

Віднесення відомостей до державної таємниці — це важлива складова державної економічної політики. Встановленням обмежень доступу до відомостей, що становлять державну таємницю в галузях науки, науково-дослідних, дослідно-конструкторських робіт, промислового виробництва, звужуються сфери застосування цієї інформації. Особливо це стосується такої чутливої сфери, як технології подвійного призначення, нові види виробництва та технологічні процеси, що мають важливе не лише оборонне, а й загальне значення для науково-технічного прогресу, розвитку економіки та суттєво впливають на зовнішньоекономічну діяльність. Тільки всебічне економічне обґрунтування всіх факторів дасть змогу об'єктивно оцінювати необхідність віднесення відомостей до державної таємниці на підставі економічної шкоди у разі їх розголошення та враховувати можливість переваги відкритого використання таких відомостей, а також забезпечувати раціональне використання бюджетних коштів для захисту відомостей, які справді необхідно приховувати в інтересах національної безпеки.

В умовах лібералізації економіки та ринкових відносин всебічне економічне обґрунтування необхідності і доцільності віднесення відомостей до державної таємниці — це веління часу. Такий підхід до вирішення цих питань сприятиме усуненню елементів формалізму і суб'єктивізму в цій важливій сфері державної економічної політики.

Економічне обґрунтування віднесення відомостей до державної таємниці включає ряд таких чинників, як:

— економічна шкода від розголошення відомостей, які віднесені чи мають бути віднесені до державної таємниці, у вартісному виразі;

— визначення переваг можливого відкритого використання відомостей, які віднесені чи мають бути віднесені до державної таємниці, також у вартісному виразі можливої економічної вигоди;

— визначення обсягів витрат бюджетних коштів на захист відомостей, що мають бути віднесені до державної таємниці.

При цьому слід враховувати, що кваліфікований розгляд цих чинників сприятиме позитивній оцінці можливої потенційної, реальної і попередженої економічної шкоди державі внаслідок протиправних діянь щодо державної таємниці.

Потенційна економічна шкода — це можливі матеріальні збитки держави, які можуть бути заподіяні їй внаслідок розголошення відомостей, які віднесені чи мають бути віднесені до державної таємниці. Потенційна економічна шкода є одним із важливих критеріїв віднесення відомостей до державної таємниці.

Реальна економічна шкода — це матеріальні збитки держави, заподіяні внаслідок розголошення відомостей, віднесених до державної таємниці. На підставі визначення у вартісному виразі реальної економічної шкоди до винних посадових осіб та громадян застосовуються правові (цивільно-правові, адміністративні, кримінальні) санкції за розголошення відомостей, що становлять державну таємницю, а також вживаються заходи для ліквідації негативних наслідків цих дій.

Попереджена економічна шкода — це своєчасно, запобіжними заходами ліквідовані умови для розголошення відомостей, віднесених до державної таємниці, що могли завдати матеріальних збитків державі. На підставі сукупності фактів запобігання економічній шкоді оцінюється стан захисту державної таємниці у відповідних галузях та ефективність роботи керівників державних органів, місцевого самоврядування, підприємств, установ і організацій та їхніх спеціальних підрозділів і служб щодо забезпечення захисту державної таємниці.

Можна запропонувати такий варіант обґрунтування необхідності й доцільності віднесення відомостей до державної таємниці, а саме:

Перше. Визначення нормативно-правовим документом, затвердженим Кабінетом Міністрів України, переліку сфер діяльності (об'єктів), що віднесені чи мають бути віднесені до дер-

жавної таємниці, економічна шкода від розголошення яких обґрунтовується тільки у вартісному виразі. Серед таких сфер діяльності (об'єктів) можуть бути:

- науково-дослідні, дослідно-конструкторські роботи та проектні роботи, що включаються до державного оборонного замовлення та формуються на основі державних науково-технічних програм, рішень Президента України та постанов Кабінету Міністрів України, спрямованих на забезпечення потреб оборони і безпеки держави;

- оборонне замовлення на підготовку виробництва власного озброєння і військової техніки, що формується на основі завершених дослідно-конструкторських робіт або робіт, що є на етапі розробки робочої документації;

- наукові, науково-дослідні, дослідно-конструкторські та проектні роботи подвійного призначення, на базі яких можуть бути створені прогресивні технології, нові види виробництва продукції та технологічні процеси, що мають не тільки оборонне, а й важливе значення для науково-технічного прогресу, економічного розвитку країни або суттєво впливають на зовнішньоекономічну діяльність;

- спільні з іноземними партнерами науково-дослідні, дослідно-конструкторські, проектні роботи та промислове виробництво, що містить відомості, віднесені до державних і міждержавних таємниць;

- зовнішньоекономічні торговельні договори та угоди на продаж (закупівлю) продукції (об'єктів), що містять державні таємниці тощо.

Кожна із цих сфер діяльності (об'єктів) має чітко встановлене джерело, обсяги фінансування, що дає змогу без застосування умовних одиниць (балів) визначити економічну шкоду (потенційну, реальну або попереджену) в фактичному економічному вираженні.

Наприклад. Приватне підприємство розробило прогресивну технологію, що дає змогу організувати новий вид виробництва наукоємної конкурентоспроможної продукції. За ініціативою цього підприємства державним експертом з питань таємниць ця прогресивна технологія була віднесена до державної таємниці. На підставі договору з відповідним державним органом приват-

не підприємство передало цю технологію у володіння і розпорядження держави. Власникові (розробнику) технології відшкодування його витрат склали згідно з договором 5 млн. грн. На створення промислової бази виробництва нової продукції було витрачено 10 млн.грн. Водночас ще до закінчення підготовки промислового виробництва власник технології, як було встановлено, передав її іноземному конкуренту. Останній, маючи більші економічні можливості, вже опанував ринки, що прогнозувалися для використання вітчизняними виробниками. У даному випадку втрачається сенс для розгортання виробництва у запланованих обсягах. Економічна шкода від розголошення відомостей, віднесених до державної таємниці (передача іноземному конкуренту), обраховується без будь-якої формули.

А якщо використовувати формулу, за якою²⁷⁵:

W_{ek} — показник, що характеризує економічну шкоду;

W_j — показник, що характеризує виділені кошти для розробки і створення об'єкта (у даному випадку наукоємної продукції);

W_2 — показник, що характеризує використання коштів у разі розголошення відомостей, віднесених до державної таємниці, то у випадках, коли наслідком передачі прогресивної технології іноземному конкуренту буде повне згортання нового промислового виробництва, економічна шкода становитиме:

$W_{ek} = 5 \text{ млн.} + 10 \text{ млн.}$, де: 5 млн. — це відшкодування розробникові прогресивної технології, віднесеної до державної таємниці; 10 млн. — це витрати держави на створення промислової бази виробництва нової продукції.

У випадках, коли передача прогресивної технології іноземному конкуренту впливає лише на обсяги виробництва, а не на повне його згортання або ліквідацію, доцільно від загальної вартості економічної шкоди відрахувати відсоток, на який зменшується виробництво.

Ще один приклад. Відповідно до ЗВДТ відомості, що містяться в директивах, планах та вказівках делегаціям і посадовим особам, які представляють Україну на переговорах, у тому числі із зовнішньоекономічних питань, становлять державну таємницю²⁷⁶. Невжиття необхідних заходів для збереження в таємниці

планів і намірів щодо укладання зовнішньоекономічної торговельної угоди з іноземною державою, про які стало відомо конкурентам, може спричинити тяжкі наслідки, серед яких:

- зрив укладання торговельної угоди на продаж іноземній державі української продукції, при цьому економічна шкода дорівнюватиме вартості запланованих обсягів продажу продукції;

- компрометація конкурентами української продукції, наслідком чого буде зменшення ціни на її продаж. Економічна шкода дорівнюватиме відсотку зниження цін на продаж загальних обсягів продукції.

Друге. Для обґрунтування підстав віднесення відомостей до державної таємниці у сферах діяльності, відповідно до запропонованого переліку, потрібно всебічно обґрунтувати можливі переваги відкритого використання цих відомостей. Серед факторів, які варто враховувати, є такі, як:

- отримання значного економічного ефекту від широкого відкритого використання цих відомостей;

- забезпечення науково-технічного прогресу у відповідних галузях економіки;

- освоєння зовнішніх ринків та зміцнення позицій на них України.

Окрім того, може розглядатися і політична доцільність відкритого опублікування і використання відомостей, що підлягають віднесенню до державної таємниці.

Механізм обґрунтування можливих переваг відкритого використання відомостей, що підлягають віднесенню до державної таємниці, у конкретних сферах діяльності може бути визначений запропонованим нормативно-правовим документом, затвердженим Урядом України. Правовими нормами цього документа розгляд питань щодо можливої переваги відкритого використання відомостей доцільно покласти на науково-технічні ради державних органів — замовників і виконавців робіт. Альтернативним варіантом може бути покладання таких обов'язків на експертні ради з проведення наукової і науково-технічної експертизи проектів міждержавних, державних і національних програм, які створюються і діють відповідно до порядку і правил, встановлених Законом України «Про наукову і науково-технічну експертизу»²⁷⁷. Висновки за результатом розгляду питань про можливі переваги відкритого використання відомостей,

що підлягають віднесенню до державної таємниці, надсилаються відповідному експерту з питань таємниць.

Державний експерт приймає рішення про віднесення відомостей до державної таємниці з урахуванням висновку про можливі переваги відкритого використання цих відомостей. Відповідно до світової практики необхідність і доцільність віднесення відомостей до державної таємниці вирішується на підставі такого принципу, а саме: у випадках, коли переваги відкритого використання цих відомостей перевищують можливу шкоду від їх розголошення (витік, передача та тощо), вказані відомості не належать до державної таємниці. Надалі така інформація використовується як відкрита або службова, згідно з рішенням відповідних державних органів до сфери відання яких вона належить.

При цьому слід враховувати те, що в деяких випадках, зумовлених інтересами забезпечення національної безпеки, а іноді, виходячи із політичної доцільності, відомості щодо окремих сфер діяльності, незважаючи на переваги відкритого використання, можуть бути віднесені до державної таємниці.

Визначення підстав для віднесення відомостей до державної таємниці, з урахуванням переваг можливого відкритого використання, є важливим аспектом економічного підходу до вирішення цих питань.

Третє. Важливе значення для обґрунтування підстав щодо віднесення відомостей до державної таємниці має визначення витрат на захист цих відомостей.

Нагадаємо, що Методичні рекомендації, на підставі яких визначаються критерії віднесення відомостей до державної таємниці, не враховують цього показника. Значення показника, який характеризує обсяги та ефективність використання виділених коштів для створення та забезпечення функціонування сфери діяльності (об'єкта), наводиться без урахування витрат на організацію режимно-секретної роботи, пов'язаної з захистом цих відомостей²⁷⁸.

У світовій практиці, а також у колишньому СРСР, в якому характерним було тотальне засекречування, діяв такий принцип: якщо витрати на захист відомостей, що розглядаються на предмет віднесення до державної таємниці, перевищують можливу шкоду від їх розголошення, то такі відомості не підлягали

віднесенню до категорії державної таємниці. Ці відомості використовувалися як службова (військова) таємниця або як відкрита інформація відповідно до рішень державного органу, у віданні якого вони перебували. Безумовно, в таких випадках також були винятки, пов'язані з політичною доцільністю та іншими інтересами, з урахуванням яких відомості відносилися до державної таємниці і захищалися, незважаючи на витрати на режимно-секретне забезпечення.

Державна таємниця — це відомості, власником яких є держава, або відомості, які в установленому законодавством порядку передаються у власність держави від інших суб'єктів України в інтересах забезпечення національної безпеки. Фінансування витрат на діяльність, пов'язану з державною таємницею, та забезпечення їх захисту здійснюється за рахунок коштів державного бюджету. Кошти у відповідних бюджетах передбачаються окремим рядком. А на підприємствах, в установах і організаціях, незалежно від форм власності, витрати на режимно-секретне забезпечення відносяться до собівартості продукції. Фінансує їх замовник секретних робіт також із бюджетних або позабюджетних державних коштів.

Витрати на захист відомостей, віднесених до державної таємниці з урахуванням ступеня їх секретності, включають витрати за рахунок державних коштів матеріально-технічних, трудових, фінансових ресурсів, а також відповідну компенсацію працівникам за роботу в умовах режимних обмежень.

Нагадаємо, що ступінь секретності інформації, що характеризує її важливість, визначає рівень охорони відомостей, віднесених до державної таємниці. При цьому слід підкреслити особливо, що режимно-секретне забезпечення починається з обрахунків витрат необхідних ресурсів на захист цих відомостей. Рациональність витрат залежить від всебічно обґрунтованої необхідності і доцільності включення відомостей до цієї категорії та хоча б мінімально необхідних ресурсів для режимно-секретного забезпечення.

Для забезпечення захисту відомостей, віднесених до державної таємниці, тобто організації всього комплексу режимно-секретної роботи в державних органах, на підприємствах, установах і організаціях, в яких вперше розпочинається діяльність,

пов'язана з державною таємницею, потрібно обрахувати необхідні ресурси та витрати на них, а саме:

- чисельність режимно-секретного органу, до складу якого можуть входити підрозділи: режиму, секретного діловодства, технічного, за необхідності криптографічного захисту інформації (підррахунки здійснюються, виходячи із обсягів робіт, пов'язаних з державною таємницею);

- категорії і чисельність посадових осіб, яким відповідно до службової необхідності оформляється допуск і надається доступ до державної таємниці (доцільно враховувати загальну кількість посадових осіб і кількість працівників для виконання технічних робіт щодо оформлення матеріалів на допуск та надання доступу до відповідних відомостей);

- організація фізичної охорони і пропускного режиму та інженерно-технічної охорони виділених приміщень для виконання секретних робіт та зберігання документів та інших носіїв такої інформації;

- організація технічного захисту інформації (за необхідності — криптографічного). При цьому враховуються витрати на придбання засобів технічного захисту виділення приміщень, каналів зв'язку, інформаційно-телекомунікаційних систем та технічних засобів обробки інформації;

- витрати на підготовку та підвищення кваліфікації працівників режимно-секретних органів та інших підрозділів і служб, що створюються для забезпечення захисту інформації в процесі робіт, пов'язаних з державною таємницею;

- розробку внутрішніх нормативних документів (інструкції, правила, положення, методики, пам'ятки тощо), що регламентуватимуть процеси діяльності, пов'язаної з виконанням секретних робіт (підрховуються обсяги робіт, на основі яких встановлюється необхідна кількість працівників для їх розробки і впровадження);

- компенсація працівникам, що постійно працюють з відомостями, віднесеними до державної таємниці, за роботу в умовах режимних обмежень.

- забезпечення необхідним інструментарієм та обладнанням режимно-секретних органів інших підрозділів і служб, а також посадових осіб для виконання, покладених на них робіт, пов'язаних з державною таємницею.

Для обрахунків витрат на захист відомостей, віднесених до державної таємниці, залучаються спеціалісти режимно-секретних органів, інших спеціальних підрозділів і служб, що створюються для захисту такої інформації, а також планово-економічних підрозділів. А в установах, організаціях і на підприємствах, де виконуються дослідження, розробки і здійснюється промислове виробництво продукції для вказаних обрахунків, залучаються і спеціалісти підрозділів — безпосередніх виконавців секретних робіт.

У державних органах та органах місцевого самоврядування витрати на режимно-секретні роботи щодо забезпечення захисту державної таємниці доцільно визначати окремим рядком у кошторисах витрат на утримання цих органів.

На підприємствах, в установах і організаціях, в яких виконуються дослідження, розробки і промислове виробництво продукції відповідно до державних замовлень, доцільно розробляти калькуляцію вартості режимно-секретних заходів, на підставі якої витрати включають до собівартості продукції в договорі із замовником робіт.

Нами розглянуто варіант визначення витрат на режимно-секретне забезпечення захисту державної таємниці для випадку, якщо такі роботи виконуються вперше. У державних органах, а також на підприємствах, установах і організаціях, незалежно від форми власності, у разі збільшення обсягів робіт, пов'язаних з державною таємницею, доцільно проводити відповідно до наведеного переліку витрат розрахунки необхідних додаткових матеріально-технічних, трудових і фінансових ресурсів для забезпечення виконання поставлених завдань. У госпрозрахункових установах, організаціях і підприємствах це питання підлягає регулюванню договором із замовником робіт.

Фінансування заходів, необхідних для захисту відомостей, віднесених до державної таємниці, — це важлива стаття витрат бюджетних коштів. Розробити кошторис витрат, калькуляцію робіт щодо режимно-секретних заходів та визначити їх вартість може тільки безпосередній виконавець секретних робіт відповідно до їх обсягу (державний орган), а також виконавець досліджень на підставі державного замовлення з урахуванням реальних умов, в яких виконуватимуться ці роботи. У зв'язку із наведеним виникають деякі проблеми.

Рішенням державного експерта з питань таємниць визначається обсяг фінансування заходів, необхідних для охорони інформації, яка цим рішенням віднесена до державної таємниці²⁷⁹. Державний експерт реально може визначити такі обсяги фінансування тільки стосовно конкретних науково-дослідних, дослідно-конструкторських і проектних робіт на підставі пропозицій підрядника або виконавця цих робіт.

У інших випадках, коли приймається рішення про віднесення відомостей до державної таємниці в узагальненому вигляді, таке рішення державного експерта матиме лише формальне навантаження.

Наприклад, відомості про технології подвійного призначення, що мають перевагу порівняно з кращими зарубіжними аналогами²⁸⁰; відомості про мету, напрями, науково-технічні ідеї та можливість впровадження (реалізації) фундаментальних та пошукових прикладних наукових досліджень в інтересах оборони України²⁸¹. Ці відомості рішеннями відповідних державних експертів віднесені до державної таємниці і включені до ЗВДТ. Вони розпорошені по різних галузях, відомствах, установах і організаціях, розробляються і зберігаються в різних умовах. Враховувати все це, визначити обсяги фінансування для їх захисту державний експерт практично не спроможний.

Таким чином, доцільно, щоб державний експерт персонально відповідав за визначення обсягів фінансування заходів захисту відомостей безпосередньо у сфері, де він працює. Стосовно конкретних робіт, що розміщуються у підрядника, доцільне всебічне врахування державним експертом пропозицій щодо вартості режимно-секретних заходів, які мають надаватися виконавцями цих робіт.

Для визначення у Державному бюджеті України, бюджеті Автономної Республіки Крим та місцевих бюджетах окремим рядком коштів на здійснення діяльності, пов'язаної з державною таємницею, потрібно розробити і впровадити механізми формування вказаних статей відповідних бюджетів.

Сьогодні рішення державного експерта щодо обсягів фінансування режимно-секретних заходів мають лише рекомендаційний характер. Фінансування заходів на здійснення режимно-секретної діяльності у Державному бюджеті України визначається законодавцем. Розпорядником щодо витрат бюджетних коштів

є Уряд України. Державні органи мають здійснювати витрати на забезпечення захисту державної таємниці лише в межах, визначених відповідними рішеннями Кабінету Міністрів України. У зв'язку з цим механізми формування відповідних статей Державного бюджету України потрібно встановити нормативним документом, затвердженим Кабінетом Міністрів України. Цей документ мав би включати:

- порядок і правила обґрунтування державними експертами з питань таємниць необхідності і доцільності віднесення відомостей до державної таємниці з урахуванням усіх зазначених чинників (економічної шкоди, інших тяжких наслідків від розголошення, можливих переваг відкритого використання таких відомостей, прогнозованих витрат бюджетних коштів на захист цих відомостей);

- порядок надання пропозиції державних органів (центральных, регіональних і місцевих) щодо обсягів фінансування робіт, пов'язаних з державною таємницею, що реально виконуються;

- правила обрахунків і порядок надання пропозицій державними органами щодо обсягів фінансування режимно-секретного забезпечення державного замовлення на наступний рік, що оформляється відповідно до постанови Кабінету Міністрів України «Про порядок формування, розміщення та виконання державного замовлення для забезпечення потреб оборони і безпеки» від 28 вересня 1996 року, № 1194;

- визначення термінів подання пропозицій про обсяги фінансування заходів забезпечення захисту державної таємниці, які відповідали б термінам розробки проекту Державного бюджету України на черговий календарний рік;

- визначення державного органу, відповідального за узагальнення пропозицій щодо обсягів фінансування із Державного бюджету України заходів захисту відомостей, віднесених до державної таємниці, та подання цих пропозицій у встановлений строк до Кабінету Міністрів України.

Таким чином, розв'язання зазначених проблем щодо віднесення відомостей до державної таємниці та їх засекречування потребують подальшого вдосконалення чинної нормативно-правової бази, а саме: реалізації в цій сфері діяльності принципів обґрунтованості і своєчасності; економічної необхідності і доцільності віднесення відомостей до державної таємниці з урахуван-

ням економічної шкоди, інших тяжких наслідків від їх розголошення, можливих переваг їх відкритого використання та витрат на забезпечення захисту таких відомостей, що доцільно визначати правилами і процедурами, які затверджує Уряд України.

Окремо підлягають розгляду проблеми, пов'язані з віднесенням відомостей до інших передбачених законом таємниць, конфіденційної інформації та критерії визначення їх конфіденційності.

На сьогодні віднесення відомостей до інформації з обмеженим доступом, що не становить державної таємниці, здійснюється на підставі відомчих методик, різних за змістом щодо вимог, критеріїв і процедур. А в окремих випадках ці питання вирішуються на підставі методик радянських часів. Тобто практично розробити методіку віднесення відомостей до інформації з обмеженим виступом, що не становить державної таємниці (крім банківської) на підставі правових норм неможливо через їхню відсутність. Вирішення цих питань можливе лише на основі узагальнення накопиченого досвіду в державних органах, на підприємствах, в установах і організаціях.

Ще однією проблемою є визначення повноважень посадових осіб щодо віднесення відомостей до інформації з обмеженим доступом, яка не становить державної таємниці. Стосовно державної таємниці такі повноваження надані тільки державному експерту з питань таємниць. На державних підприємствах, в установах і організаціях мають місце непоодинокі факти одноосібного прийняття рішень про віднесення відомостей до конфіденційної інформації відповідними керівниками. У більшості підприємств, установ і організацій пропозиції щодо переліку такої інформації розробляються експертними комісіями (склад від 3 до 7 осіб) на підставі пропозицій структурних підрозділів. Цей перелік затверджується керівником підприємства, установи, організації.

Визначення підстав для віднесення відомостей до конфіденційних доцільно здійснювати за методикою, запропонованою для державної таємниці, а саме:

- визначення можливих збитків у разі несанкціонованого поширення конфіденційних відомостей;

- обґрунтування факторів щодо можливих переваг відкритого використання включених відомостей;

— визначення матеріально-технічних, трудових, фінансових витрат для забезпечення захисту відомостей, включення самих витрат до переліку конфіденційної інформації.

Можливі збитки (школа) від несанкціонованого поширення цих відомостей (моральні, матеріальні, фінансові тощо) оцінюються в кількісних (вартісних) і якісних показниках. Кількісні (вартісні) показники можливих збитків, як правило, пов'язані з рівнем зниження виробничої, торговельної, фінансової діяльності. Якісні показники пов'язані з моральними та іншими негативними наслідками, що не піддаються економічному обґрунтуванню в реальному вартісному вираженні.

Визначенням витрат на захист відомостей, що включають до переліку конфіденційної інформації, здійснюється обрахування у вартісному вираженні всього комплексу заходів і засобів забезпечення режиму конфіденційності з урахуванням умов діяльності державного органу, підприємства, установи, організації.

До переліків конфіденційної інформації включаються, як правило, відомості, для яких величина моральних, матеріальних і фінансових збитків від несанкціонованого поширення перевищує підсумовані показники від їхнього відкритого використання і витрат на захист таких відомостей.

До переліків конфіденційної інформації, звичайно, включається графа, в якій вказується термін обмежень доступу до інформації, що містить цей перелік. У зв'язку з невизначеністю на рівні актів законодавства термінів обмеженості, що встановлюються для інформації з обмеженим доступом, на практиці це робиться в такий спосіб: 1) у спеціальній графі проти кожного пункту переліку встановлюється термін дії обмежень доступу, тобто графа конфіденційності; 2) встановлюється загальний термін дії обмежень для всіх пунктів переліку. Після закінчення встановлених термінів дії обмежень доступу відомості передаються для відкритого використання або встановлюється (продовжується) новий термін дії грифу конфіденційності.

Розглянутий комісією перелік конфіденційної інформації підписується членами експертної комісії (у деяких випадках — головою і секретарем цієї комісії) і затверджується керівником державного органу, підприємства, установи, організації.

Таким чином, удосконалення системи віднесення відомостей до інформації з обмеженим доступом, що не становить дер-

жавної таємниці, може бути здійснене лише на підставі правового регулювання відносин, пов'язаних з правовим режимом кожного виду такої інформації.

Інформація та бізнес є нерозривними поняттями. Більш того, останнім часом бізнес став набувати властивостей похідної величини від вміння знаходити, обробляти та використовувати інформацію. Слова «хто володіє інформацією, той володіє світом» наповнились практичним змістом. Бізнес став сам себе постачати, планувати та продавати. Конкуренція, що загострюється при цьому, необхідність знання ринкової кон'юнктури, проведення маркетингових досліджень, активне просування пропозицій щодо високотехнологічної продукції, створення товаропровідних мереж, дилерських майданчиків, дистриб'ютерських центрів тощо — все це вимагає інформації, надійної, вірогідної, якісної, постійно поновлюваної. Інформаційний ринок має стати для цього прозорим, але не вистачає досвіду роботи з інформацією, що перейшла від «загальнодержавної» до категорії товару, стала об'єктом власності різних суб'єктів. Ми часто не в змозі зрозуміти сутність інформаційних проблем сьогодні, тим більше зазирнути у завтра. Це веде українських науковців, створювачів науково-технічної продукції, бізнес до ролі доганяючого, а сам процес вже набирає усталеності і, тим самим, змушує відтворювати це відставання.

Конкретні досягнення, конкретний бізнес існують у визначеному економічному, політичному, соціальному і технологічному контексті. Відповідним чином організована інформація впливає на об'єктивний розвиток суспільства, формує стратегічні та тактичні рішення економічного поступу, є його системним підґрунтям.

* * *

В Україні з її значним науково-технічним і творчим потенціалом, загалом є усвідомлення того, що продукти інтелектуальної діяльності — це реально діючий капітал. Водночас «тінізація» інформаційної складової щодо цього капіталу, неврегульованість на правовому і організаційному рівнях реалізації науково-технічної політики призводять до зниження оцінки і можливостей наукового потенціалу, його малоефективності при здійсненні економічних перетворень, що мають інноваційний характер.

Підвищення ефективності інформаційної складової науково-технічної політики держави в економічному і соціальному розвитку безпосередньо залежатиме від регулюючої і координуючої ролі держави щодо формування централізованих (державний сектор) та децентралізованих (приватний сектор) потоків змістовних інформаційних ресурсів за результатами науково-технічної діяльності, які суттєво впливають на рівень і загальний стан економіки України. Потребує вдосконалення законодавча і нормативно-правова база та здійснення певних організаційних заходів щодо державного управління національними інформаційними ресурсами. Підлягають вдосконаленню правові механізми реалізації права власності на ЗІР та об'єкти інтелектуальної власності та їхнього активного залучення до господарського обігу, в тому числі через цивілізовану їх комерціалізацію. Потребує цілеспрямованого розвитку інформаційна інфраструктура країни та інформаційна індустрія щодо надання інформаційних продуктів та послуг як важливі умови інтеграції національного інформаційного простору в світові інформаційні структури. Доцільна розробка на державному рівні правових та організаційних заходів щодо формування національної системи НТІ з чітким визначенням центральної і регіональної організаційних структур, принципів і напрямів діяльності з питань формування єдиного розподіленого фонду НТІ за результатами науково-технічних досліджень, у тому числі й закритої тематики, та матеріально-технічної та фінансової підтримки його функціонування, використання та захисту.

В умовах реструктуризації власності забезпечення ефективного використання національних ресурсів, зокрема ЗІР, потребує першочергового розв'язання таких проблем:

— на основі законодавчого визначення правового режиму кожного виду інформації забезпечити впровадження правових механізмів реалізації прав фізичних, юридичних осіб і держави на інформацію та встановити повноваження і відповідальність суб'єктів України за формування і ефективне використання національних інформаційних ресурсів, у тому числі ЗІР, як для економічного і соціального розвитку країни, так і для забезпечення рівноправного їх використання у процесі міжнародного інформаційного обміну;

І — розробити і впровадити економічні механізми формування і використання ЗІР за результатами науково-технічної діяльності з внесенням необхідних змін і доповнень до державної податкової, фінансово-кредитної, інвестиційної політики тощо та здійснити відповідне коригування системи фінансування державних замовлень на ЗІР, спрямованих на економічний і соціальний розвиток та стале функціонування системи національної безпеки України;

— вжити заходів для припинення бурхливого і стихійного формування інформаційного ринку. Політику ціноутворення на інформаційні ресурси, в тому числі ЗІР, на законодавчому рівні визначити як важливу складову державної цінової політики із впровадженням правових, організаційних і економічних механізмів впливу на ринкові процеси щодо цієї сфери;

— на основі вдосконалення правових засад та оптимізації структури державних органів створити загальнодержавну систему захисту інформаційних ресурсів з обмеженим доступом та важливою для суспільства і держави відкритої інформації; розвиток національної складової мережі Інтернет та корпоративних інформаційних систем здійснювати тільки із застосуванням всього комплексу заходів і засобів для захисту інформації, що підлягає охороні з боку держави та проведенням атестації інформаційних систем спеціально уповноваженим державним органом на їх відповідність вимогам щодо захисту інформації.

Необхідною умовою економічного зростання окремих регіонів і цілих країн є чітке визначення пріоритетних напрямів дій держави з прискорення комерційного використання результатів наукових досліджень, що фінансуються урядом, стимулювання співпраці між партнерами з промисловості і науковими установами та науковцями. Створення засад інформаційного суспільства є шляхом для стимулювання бізнесових кіл щодо сприйняття можливостей використання сучасних інформаційно-комунікаційних технологій для відтворення науково-технічного потенціалу, ефективного використання ЗІР у процесі як внутрішньої, так і зовнішньоекономічної діяльності. Особливої уваги заслуговують питання, пов'язані з централізованим формуванням та обробкою інформаційних ресурсів вітчизняного та зарубіжного походження, у тому числі комерційного та обмеженого поширення, що становлять інтерес для промислової та зовнішньоеко-

номічної діяльності держави. Найбільш прийнятним варіантом їх вирішення може бути вдосконалення наявної системи НТІ України як основи інформаційної інфраструктури держави. Нагальною необхідністю є проведення аналізу ЗІР з науково-технічної діяльності, створених у кооперації із науковими установами і підприємствами республік колишнього СРСР, що перебувають у спецфондах галузей, підприємств та установ калькодержальником яких є Російська Федерація. Метою аналізу мають бути: оцінки їх корисності для наукової, промислової, конверсійної, бізнесової, зовнішньоекономічної діяльності; доцільність збереження обмежувальних грифів з урахуванням сучасного стану і тенденцій розвитку відповідних галузей науки, техніки і технологій, а також строків встановлення обмежень доступу; визначення порядку подальшого використання цих матеріалів для економічного і соціального розвитку країни.

Удосконалення правових механізмів та організаційних заходів з забезпечення комерційного використання інформаційних ресурсів за результатами науково-технічної діяльності у сучасних умовах має передбачати вирішення таких питань, як:

- правового оформлення об'єкта ринкових відносин — змістовного інформаційного ресурсу держави (відкриття, винаходи, корисні моделі, промислові зразки, товарні знаки, ноу-хау тощо) шляхом вдосконалення правових механізмів інститутів власності, патентного і авторського права, права власності на інформацію обмеженого доступу. Метою змін і доповнень до чинного законодавства має бути забезпечення прав власника і володаря ЗІР на отримання відповідних доходів та ефективний захист цих прав як на внутрішньому, так і світовому ринках;

- розробки нормативних, методичних і технологічних основ організації та спільного використання документальних фондів, що створювалися та створюватимуться за результатами науково-технічної діяльності з урахуванням правового режиму кожного виду ЗІР;

- визначення на державному рівні єдиної організаційної структури, порядку і правил матеріально-технічного та фінансового забезпечення щодо створення, підтримки, надання в обіг та використання інформаційного ресурсу України за результатами науково-технічної діяльності як стратегічного ресурсу держави.

Формування нової економічної системи, ринкових відносин як внутрішніх, так і з оточуючим нас середовищем з використанням інформаційних ресурсів, що підлягають захисту, потребує вдосконалення системи віднесення відомостей з науково-технічної діяльності, об'єктів інтелектуальної (промислової) власності до інформації з обмеженим доступом. Наукові здобутки, новітні технічні і технологічні рішення, ноу-хау тощо завжди визначали прогресивний економічний і соціальний розвиток та стале функціонування системи національної безпеки. Тому віднесення відомостей, передусім з науково-технічної та економічної діяльності, до інформації з обмеженим доступом має стати важливою складовою державної економічної політики. Правила вирішення цих питань мають враховувати як сукупні збитки від витоку і розголошення таких відомостей, так і можливі вигоди від їх відкритого використання та збереження бюджетних коштів, як витрачаються на захист такої інформації.

Розділ 3

СТРАТЕГІЯ УПРАВЛІННЯ НАЦІОНАЛЬНИМИ ІНФОРМАЦІЙНИМИ РЕСУРСАМИ ТА ШЛЯХИ ЇЇ ВДОСКОНАЛЕННЯ

3.1. Інституційний характер формування і використання змістовного інформаційного ресурсу з наукового потенціалу України

Широке використання інформаційних технологій у різних сферах життєдіяльності, суттєво змінило уявлення про місце і роль інформації в сучасному суспільстві, дедалі виразніше виявляється нова суспільно-економічна категорія — національні інформаційні ресурси набули ознак стратегічних, стали важливим чинником розвитку постіндустріального світу. Можна з упевненістю говорити про те, що національний, соціальний, культурний престиж держави, її економічне становище визначаються рівнем накопичення та використання національних інформаційних ресурсів.

Було б спрощенням вважати інформацію лише предметом купівлі-продажу. Намагання прямо застосовувати грошовий еквівалент інформації здебільшого ускладнює відображення її справжньої соціальної та ринкової цінності²⁸². В умовах становлення інформаційного ринку поняття «інформаційний капітал» може відображати втрати та надбання у грошовому еквіваленті щодо процесів відтворення, накопичення, зберігання та використання змістовних даних та відомостей, що становлять змістовний інформаційний ресурс країни. Це особливо важливо сьогодні тому, що інформація, представлена фондами першоджерел, баз даних, архівів тощо, ще не стала в Україні економічно вагомим. Її балансова вартість переважно відображає лише вартість матеріальних носіїв та / або вартість технічних за-

собів, на яких вона зберігається²⁸³. Такий стан може призвести до багатьох негативних наслідків: встановлення спекулятивних або демпінгових цін на інформацію, безконтрольного розпродажу — інформації з державних фондів, організації приватного бізнесу з використанням державних інформаційних ресурсів, нееквівалентного бартеру, втрати прав на інформацію, неконтрольованого витоку (вивезення) вітчизняних інформаційних ресурсів, ухилення від оподаткування при продажу інформаційних продуктів та послуг тощо²⁸⁴.

Розвиток соціально-економічних систем відбувається через розвиток інституцій, які й персоніфікують національні економіки. Не менш важливе значення має обґрунтування, передусім теоретичне, системи національних інформаційних ресурсів — СНІР як такої, її сутності, структури, внутрішнього змісту і тих складових, що забезпечують її функціонування і розвиток. Досягнення мети трансформації забезпечується активною позицією державної інформаційної політики України, що потребує чітко визначеної орієнтації на задіяння СНІР в економіці країни, що дає змогу спільноті звернути увагу на позитивні аспекти цієї системи, створити можливість для їх впровадження та якнайширшого застосування, загальмувати негативні моменти.

За таких умов одним із головних державних завдань стає координація зусиль, пов'язаних з інформаційною підтримкою науково-технічного розвитку галузі, державної акредитації центрів науки, освіти та високих технологій.

Економічний потенціал України сьогодні має більшою мірою визначатися рівнем розвитку інформаційної інфраструктури, тому зростає загроза потенційної вразливості економіки щодо інформаційного впливу²⁸⁵.

Інституційно СНІР (а в її межах — змістовний інформаційний ресурс) існує в певному політичному та економічному полі, а тому її становлення передбачає наявність відповідних правових та організаційних утворень, за яких система конкретизується і пристосовується до умов реформування економічного устрою пострадянських країн.

Зрозуміло, що передбачити повною мірою модель економічного розвитку України просто неможливо, її формування — це поступовий і довготривалий процес. На сьогодні вже маємо

кілька конкретних визначень майбутньої моделі економічного розвитку України. Зокрема, що економіка України має бути ринково орієнтованою, соціально спрямованою, що однією з центральних проблем економічної політики є переосмислення місця і ролі держави у цих процесах, що держава може звільнити економіку від своєї присутності тільки там, де сформовано й ефективно діють повноцінні ринкові механізми²⁸⁶. Б. Панасюк називає її соціальною ринковою економікою²⁸⁷, С. Мочерний вважає, що адекватною умовам України є модель «народної економіки»²⁸⁸, І. Кравченко обґрунтовує необхідність побудови «української кооперативної держави». В. Черняк²⁸⁹ вважає, що модель економіки характеризується співвідношенням: 1) форм власності і заснованих на них секторів економіки або закладів господарювання; 2) ринкових механізмів і державного регулювання (плану і ринку); 3) централізму і децентралізму в управлінні економікою; 4) конкуренції і монополізму; 5) лібералізованості і соціальної орієнтованості економіки. Залежно від поєднання цих складових, їх системної взаємодії у світі існують різні моделі економіки. Умовно В. Черняк класифікує їх за такими угрупованнями: лібералізована економіка (США), соціально орієнтована економіка (ФРН), держава добробуту (Швеція), східно-азійська модель (Японія). Їхня сутність визначається ступенем присутності та роллю держави в економіці²⁹⁰.

Держава може забезпечувати соціально-економічний розвиток, координацію діяльності учасників економічних відносин, тільки маючи у своєму розпорядженні великі матеріальні та грошові ресурси, маючи право власності на значні ресурси та організовуючи на таких засадах великий державний ринок²⁹¹. Тому, констатує В. Мамутов, уроки реформ з формування моделі соціально-економічного розвитку свідчать, що багато рішень залежать від того змісту, який ми бачимо в таких поняттях, як свобода, з одного боку, та порядок — з іншого; тобто маємо забезпечити соціально-економічне зростання шляхом розумного поєднання ринкового саморегулювання та державного регулювання²⁹².

Економічна система, що існувала у нас раніше, характеризувалася поряд з іншими чинниками високим рівнем централізації управління економікою. Неможливо відразу і повністю відмовитися від централізму і перейти до децентралізму, тим

більше на рівні держави *in toto*. Це відбувається поступово, через пошуки ефективного співвідношення між ними, з урахуванням головної системоутворюючої ланки, якою є власність. Це положення поширюється на всі сфери соціально-економічної побудови, в тому числі на інформаційну сферу, зокрема систему національних інформаційних ресурсів.

Суперечливий характер перехідної економіки створює певні методологічні труднощі в дослідженнях процесу визначення пріоритетів інформаційної політики, коли закономірності майбутнього виводяться із сьогоденних тенденцій. Зафіксовані ж на даний момент особливості розвитку у майбутньому можуть виявитися специфічними рисами кризового стану суспільства. При цьому помилковість вибору пріоритетів може обійтися дуже дорого, оскільки йдеться про великі інвестиційні ресурси, що спрямовуються не тільки безпосередньо в інформаційну сферу, а й через використання СНІР — у всі сфери (або у переважну більшість) економіки країни.

Приклади світової практики вибору пріоритетів розвитку економіки в аспекті науково-технічного прогресу також залежать від ряду чинників. Так, на думку американських фахівців, саме інформаційні ресурси країни у остаточному підсумку визначають її можливості щодо прийняття стратегічних рішень у галузі економічної конкурентоспроможності, оборони, енергетичної незалежності. Зокрема, можливості США з отримання та ефективного використання інформації, а також збереження її конфіденційності (чи таємності), як вважають, компенсують навіть такі кроки, як скорочення збройних сил. У зв'язку з цим бази даних науково-технічної інформації належать у США до ресурсів стратегічного характеру²⁹³.

Це спонукає по-новому розглянути роль інформаційних органів різних рівнів та їхнього призначення при здійсненні ними функції поширення ЗІР, впливу на інформаційну структуру суспільства в цілому.

Особливої уваги вимагає розгляд системи управління ЗІР у зв'язку з відтворенням у ньому науково-технічних здобутків країни, реалізацією Концепції державної науково-технологічної політики.

Організаційні форми державної участі у розвитку наукових досліджень та управління ними склалися переважно у середині

XIX століття, хоч і до цього часу держава нерідко виступала як ініціатор, патрон чи замовник досліджень. Ідея розробки самостійної й цілісної наукової політики в розумінні цілеспрямованих і комплексних дій уряду і держави, метою яких є стимулювання наукових і технічних досліджень і використання їх результатів у політичних цілях, уперше формується у США після закінчення Другої світової війни. На перший план висувались утилітарні функції науки і, як наслідок, ідеї та принципи здійснення державної наукової політики — вирішувались у руслі прагматизму та наукової ініціативи особистості. Відтоді набуває визнання принцип безпосереднього впливу уряду на управління науковими дослідженнями, які відтепер оцінюються як національне надбання (national asset), а також на оцінку результатів досліджень. Розвиток ядерної енергетики докорінно змінює відносини між світом науки і світом політики, залучає вчених до процесу прийняття політичних рішень та водночас зорієнтовує владу на включення науки до сфери державної політики²⁹⁴.

Зв'язок між світом науки і світом політики, що набув у США розвитку в роки війни, знайшов своє відображення у доповіді «Science, the Endless Frontier» («Наука, нескінченний кордон»), з якою у липні 1945 року виступив В. Буш, радник президента США Ф.Д. Рузвельта з наукових питань під час Другої світової війни). Він аргументовано довів, що специфічна природа наукових досліджень не надає можливості передбачити, де, коли, кому вони можуть виявитися корисними. Ця доповідь стала наріжним каменем розвитку наукової політики у США та інших країнах Заходу в наступні десятиліття, кожне з яких мало свої характерні особливості. Одним із наслідків окресленого підходу стало створення 1950 року Національного наукового фонду (National Science Foundation). Незабаром політична еліта Європи, її провідні політики визнають, що інвестиції у наукові дослідження — цілком виправдані та є необхідними. Було також визнано, що наукова політика має здійснюватися професійно та раціонально, на підґрунті достовірних статистичних даних і результатів компетентного аналізу. Ці висновки сприяли розвитку статистики у галузях науки і техніки, її міжнародній стандартизації («Frascati Manual», 1965) та виникненню наукометрії, пов'язаної з іменами таких дослідників, як D. de Solla Price (США)

та В.В. Налімов (СРСР). У ті ж роки виникає і напрям інформаційного забезпечення в сучасному розумінні, коли була розпочата підготовка оглядів, що містили оцінку стану та розвитку (окремих наукових дисциплін).

Відтепер пріоритет у науковій політиці отримують економічні цілі, хоч цілі, пов'язані з військовими аспектами, і надалі зберігають свою значущість.

Коли економічний розвиток не обмежувався з соціальних та економічних позицій (до 1970-х років), доцільними вважалися передусім зиски, які надавав науково-технічний прогрес. Після 1970-х дедалі більшою мірою починають враховуватися пов'язані з цим витрати та інші фактори²⁹⁵. Так, у США набувають втілення ідеї Technology Assessment (ТА) — оцінки результатів впровадження нових технологій, пов'язаних з ними реальних витрат з боку суспільства, а також можливих негативних наслідків. Розвиток популяризації науки і техніки дедалі частіше включається до комплексу заходів для здійснення державної науково-технічної політики. Стимулом щодо цього стає положення про подальший розвиток сучасної цивілізації, який може бути успішним лише за наявності відповідного рівня науково-технічної культури і не тільки у середовищі наукової та інженерно-технічної еліти, а й у найширших колах суспільства.

У країнах, які вже мали давні традиції в цій галузі, уряди беруть безпосередню участь у заходах з поширення наукових і технічних знань (Франція, Швеція) або ж надають необхідну підтримку відповідним позаурядовим організаціям (Committee for the Public Understanding of Science — COPUS, Велика Британія, Science for the People — США). Уряд Франції за сприяння регіональної влади розпочав (з 1990-х років) створення мережі центрів науки і техніки, яка на даний час налічує понад 14 центрів, що співпрацюють з Cite des sciences et de l'industrie (Paris — la Vilette). Слід підкреслити, що в СРСР, добре відстежуючи політичні аспекти розвитку науки і промисловості, насамперед у країнах Європи та США, дійшли висновку про необхідність створення системи інформаційної підтримки науки і виробництва, яка згодом, у СНД, трансформувалась із Державної системи науково-технічної інформації (ДСНТІ, 1969 рік) у систему центрів науково-технічної та економічної інформації, зокрема в Україні²⁹⁶.

У світі відбувається розуміння факту, що в міру того, як економічно розвинуте суспільство стає дедалі залежнішим від інтелектуальної діяльності (розумової праці), знань, які є результатом зусиль учених та інженерів, а також від розвитку інформаційних технологій, природничі ресурси перестають розглядатися як основний показник економічних можливостей держави. Набагато тіснішими стають взаємозв'язки науки і технології. Технологія трансформується у науку. Значно посилюються зв'язки науки і техніки з економікою. Наукова політика, як ніколи раніше, зближується з індустріальною, що згодом стає підґрунтям до зближення (а навіть і взаємопроникнення) з політикою побудови інформаційного суспільства.

Можна стверджувати, що з кінця 80-х років минулого століття відбувся перехід від наукової політики до політики науково-технічної, згодом — до інноваційної, при дедалі чіткішому окресленні науково-технічної політики як політики підпорядкування науки вимогам економіки, що й зумовило переорієнтацію академічних та посилення промислових — досліджень. Наступним витком розвитку має стати зближення науково-технічної та промислової політики з соціальною політикою, яку визначатиме роль державотворення в соціальних та глобальних процесах. Неважко зрозуміти, що за такого позитивного розвитку світового суспільства інформаційна складова державної політики набуватиме дедалі більшої вагомості.

Усвідомлюється також, що інноваційний процес значною мірою залежить від ефективної взаємодії між його учасниками — вченими університетів та промислових лабораторій, підрозділами менеджменту та маркетингу на підприємствах, ринком, від самої суті наукових відкриттів та технічних інновацій. Поряд з тематичними почали враховувати і структурні аспекти, що, зокрема, стосуються організації досліджень, підготовки до підвищення кваліфікації персоналу, забезпечення трансферу технологій від вищих навчальних закладів у промисловість, розвитку міжнародного співробітництва. Усвідомлюється і системоутворююча роль змістовних інформаційних ресурсів, що має відображення у Законі України «Про науково-технічну інформацію»²⁹⁷.

Усі ці зміни — як у межах власне науки, так і у характері її зв'язків з економікою, державою та суспільством — є взаємозумовленими. По-перше, привертає увагу взаємозв'язок про-

цесів формування державної наукової політики; розвитку методів управління наукою, по-друге, формування й поширення її впливу на інформаційну складову в науково-технічній політиці, що співвідноситься з комерціалізацією науки.

У початковий період формування державної науково-інформаційної політики в економічно розвинутих країнах важливу роль відіграли такі фактори, як створення міністерств та урядових агентств, відповідальних за координацію заходів у цій галузі", організація на загальнодержавному рівні рад з питань науки; створення системи наукового консультування у сфері управління різними секторами державної структури, до компетенції яких належала оцінка прийнятих рішень, або тих, що плануються, з використанням, за необхідності, даних експертизи та результатів відповідних досліджень, що виконувалися наукознавчими центрами тощо²⁹⁸. Як самостійні напрями державної політики в галузі науки і техніки формуються інноваційна, інформаційна політика та політика з популяризації науки і техніки.

Зокрема, становлення інформаційної політики держави відбувалося відповідно до зміни поглядів на сприяння розвитку та координації завдань науково-технологічної і промислової розбудови, найбільшими «зовнішніми» проявами якої стали:

- комп'ютеризація бібліотек і створення мереж електронної комунікації між бібліотеками, інформаційними центрами, науково-дослідними установами",

- створення бібліографічних та фактографічних баз і банків даних, включно з БД про незавершені дослідження та розробки, науково-дослідні установи із забезпеченням доступу до цієї інформації через комп'ютерні мережі, що сприяло (на перших етапах створення та функціонування) популяризації досягнень вітчизняної науки (всіх, без винятку, країн) за кордоном та вдосконаленню інформаційного обслуговування вчених у країні. Згодом саме цей напрям набуває найбільшого поширення, що прямо відповідає ринковій орієнтації економіки світового суспільства та, зокрема, процесам комерціалізації результатів наукових досліджень;

- реалізація системи віддаленого доступу до інформації про наявні в національних фондах джерела інформації, книги та часописи, в тому числі і зарубіжні;

- створення раціональних систем придбання літератури;
- організація регіональних центрів наукової і технічної інформації, а також консультативних центрів, що взаємодіяли із SME (Sales&Marketing Executive-International).

У межах цього напрямку відбувається розробка методів оцінки науки і техніки, наукові прогнозування, розвиток наукознавчих досліджень тощо. Так, розробка методів оцінки науки і техніки, наукові засади якої упродовж останніх років стали темою численних досліджень і публікацій, сприяли їх застосуванню на різних етапах, у різних формах на різних рівнях виконання майже всіх дослідницьких робіт. З 1991 року почав друкуватися і спеціальний часопис «Research Evaluation».

Попередню та заключну оцінку (в Україні — експертизу) отримують проекти досліджень і розробок, результати діяльності науково-дослідних установ і центрів, праці окремих учених і наукових колективів, наукові галузі та напрями, національні системи організації науки і техніки та управління їх розвитком. У Процесі оцінки програм організаційного характеру відбувається як зовнішнє оцінювання (стосовно місця програми^ загальному контексті політики даної установи, міністерства, уряду), так і внутрішнє (щодо ходу виконання програми та її результатів). У Франції, наприклад, питання оцінки наукових досліджень належать компетенції спеціально створеного закладу — National Evaluation Comite.

Дослідження з наукового передбачення або наукового прогнозування здійснюються у різних країнах різними способами. Водночас вони характеризуються наявністю спільних моментів, таких як систематичне вивчення та оцінка тенденцій, що спостерігаються в різних країнах і в різних галузях науки і техніки, їх зіставлення. Метою таких досліджень є надання допомоги в управлінні розвитком науки і техніки (визначення пріоритетних напрямів досліджень, тематики міжнародного співробітництва, обґрунтування стратегічних планів розвитку). При їхньому проведенні використовуються найрізноманітніші інформаційні джерела — передусім наукові й технічні публікації, аналітичні предметні огляди, застосовуються різноманітні методи досліджень, у тому числі бібліометричні та патентознавчі.

Розвиток наукознавчих досліджень як сучасна форма знань про науку, розвиток яких завжди супроводжував розвиток са-

мих наукових досліджень, проявляється у своїй найважливішій царині — дослідженнях, що стосуються наукової політики, результати яких мають слугувати засадами та передумовами політичних рішень з проблем науки. До світової інфраструктури досліджень у галузі наукової політики входять числені науково-дослідні центри, часописи (наприклад, «Research Policy»), наукові товариства та асоціації, науково-дослідні мережі, що здійснюють вивчення таких проблем світового масштабу, як наприклад, «витікання мізків» (brain-drain) або участь національних меншин у науковому прогресі. З 1990-х років при центрах наукознавчих досліджень, як правило, організовуються курси підготовки менеджерів, дослідників та адміністраторів у сфері науки.

Розвиток науково-технічної статистики як системи статистичних даних та науково-технічних показників у складі ЗІР отримує своє практичне застосування при визначенні потенціалу, ресурсів та ефективності наукового розвитку даної конкретної установи, регіону, країни. Вони дали змогу дістати уявлення про внутрішню структуру науки і техніки, їхній взаємозв'язок з економічним розвитком, про відповідність рівня розвитку науки і техніки тим цілям, які ставлять перед собою учені, наукознавці, політики та суспільство у цілому. У час швидких змін як у світовій економіці, так і в самій науці статистика та статистичні дані набувають дедалі більшого значення для контролю процесів реалізації, визначення та оцінки результатів науково-технічної політики. Треба наголосити, що таку саму роль відіграють науково-аналітичні огляди, що продукуються центрами НТІ, але вже на суттєво вищому рівні щодо предмета обстеження.

Особливо при визначенні ролі інформаційної політики слід звернути увагу на застосування оцінки технології. Її основним завданням, у світлі досвіду розвинутих країн Заходу, США, Японії, Південної Кореї, є як найбільш можливе об'єктивне дослідження позитивних і негативних результатів, обсягів витрат та корисності, що пов'язані зі здійснюваними або запланованими змінами у технології. Технологічні нововведення, що досліджуються, можуть бути широкомасштабними та принциповими або ж мати відносно вузький характер. «Оцінка технології» (Technology Assessment — TA) може стосуватися найрі-

зноманітніших сфер та галузей, які підпадають під вплив або яких торкається нова технологія: промисловості, політики, культури, захисту довкілля тощо. Предметом оцінки можуть бути, зокрема, впливи нових технологій на умови праці і довкілля (забруднення повітря, ґрунту, води), порушення прав особистості (комп'ютеризація), загрози генетичній спадковості (генна інженерія, фармакологія), катастрофи (ядерні, промислові) та ін. Оцінка технології може бути також пов'язаною з аспектами економічного та соціального розвитку, яких торкаються технологічні нововведення, таких як розвиток окремих галузей виробництва, отримання економії шляхом застосування інформаційних технологій або процеси урбанізації. Результатом цих досліджень, що ґрунтуються головним чином на збиранні відповідної інформації та її аналізі, є, як правило, доповіді та звіти, що готуються за дорученням парламентів, урядів, відомчих установ, а останнім часом — за договором з конкретними замовниками, в тому числі приватними особами. У процесі оцінки технології залежно від тематики та засобів, що є у розпорядженні аналітика (експерта чи експертної установи), можуть застосовуватися найрізноманітніші методи — від складання звичайного бібліографічного звіту і до розробок, що ґрунтуються на експертизі та моделюванні, в тому числі комп'ютерному.

Формування і розвиток наукової політики в економічно розвинутих країнах, зміни в організації управління наукою та технікою і розвиток досліджень, що забезпечують механізм управління, зміни у самому характері науки і техніки, їхніх взаємозв'язках мають своїм наслідком виникнення цілого ряду явищ як на стиках науки, техніки і виробництва, так і у сфері науково-технічної та відповідної їй інформаційної політики. У науковому середовищі, зокрема, відбувається витіснення звичних академічних норм тими, що прийняті в бізнесі, а в наукових планах відображаються цілі комерційного характеру. Широким фронтом відбувається злиття науки з виробництвом-саме в руслі комерціалізації, прийомів бізнесу.

Серед обов'язків учених академічних закладів та вищої школи дедалі більше місце посідають адміністративні та управлінські функції, а поряд з цим — усе частіше на різних етапах своєї кар'єри наукові працівники переходять на роботу до сучасних

бізнесових, бізнесово-промислових структур, стають державними чиновниками або консультантами в урядових установах. Центри досліджень і розробок у промисловості дедалі більше зміцнюють свої зв'язки з такими сферами діяльності, як наукова і технічна інформація, управління виробництвом, фінанси і маркетинг²⁹⁹.

Зміни у структурі органів управління, які відбулися після розпаду СРСР, безпосередньо відбилися саме на ланці системи органів управління державними інформаційно-змістовними ресурсами (ДСНТІ) та на відповідному механізмі захисту державної таємниці, що, врешті-решт, призвело до деформації власне координуючого начала з боку урядових структур.

З 1992 року у країні склалася ситуація, за якої система органів НТІ ще працювала і виконувала поставлені завдання, але вже не була керованою на урядовому рівні. Числені підприємства, установи та організації, пов'язані єдиним державним документообігом, опинилися по різні боки кордонів, під управлінням різних урядів, що далеко не завжди проводять доброзичливу політику. Особливо це відбулося в оборонно-промисловому комплексі.

Політичний аналіз нових глобальних проблем міжнародного розвитку, пов'язаний із впливом високих технологій у контексті «інформаційне суспільство для всіх», наданий у Всесвітній доповіді ЮНЕСКО з інформації 1997/98 (World Report Information 1997/98, UNESCO, Paris, 1998)³⁰⁰. Тематика аналітичного дослідження охоплює такі напрями міжнародного співробітництва, як³⁰¹: 1) постіндустріальна цивілізація і трансформація політичних та економічних процесів: а) динаміка розвитку глобальної інфраструктури; б) еволюція інформаційної економіки; в) міжнародна кооперація і співробітництво; г) охорона інформаційних баз даних суспільного та спеціального призначення; д) Соруایت в інформаційну добу (Н.Мур, М.Лінч, Ф.Клерк, Ш.Оппенгейм, М.Кук, Г.Вебер, Ф.Альтбах); 2) інфраструктура інформаційної індустрії: а) розвиток технологій мультимедіа; б) тенденції використання Інтернет; в) технології електронних видавництв; г) комп'ютерна індустрія (Л.Тедд, М.Вайс, Б.Кронін, Г.Фолкнер-Браун, Д.Маккейм, Ч.Чен); 3) інформаційні послуги www з метою широкого доступу та обміну базами даних бібліотек та архівів у країнах усіх географічних регіонів світу (Д.Сайсон,

А.Лібейрі, М.Ітем, О.Бутрименко, Д.Вайтелло, К.Мур, Р.Менінг, Е.Кампос, Е.Комолайф).

Розв'язання проблем світової політики в галузі комунікації, яка традиційно вироблялася на міжурядових форумах ЮНЕСКО, WIPO, МСЕ і виражала позиції всіх учасників глобального обміну інформацією, останніми роками під впливом комерціалізації інформаційного сектора перейшло до пріоритетів діяльності СОТ, яка презентує передусім інтереси розвинутих країн з потужною інформаційною індустрією. Є.А. Макаренко зазначає, що в політиці СОТ вирізняються такі принципи, як³⁰²: світова лібералізація ринків; недискримінація в міжнародній конкуренції; цивілізована участь зарубіжних агентів на національних ринках; пріоритетність приватного сектору в міжнародних відносинах.

Оскільки інформація виступає у ролі товару³⁰³, до неї відносять не тільки такі міжнародно-правові акти, як Конвенція ООН про договори міжнародної купівлі-продажу (1980 рік), а й документи, що набули останнім часом міжнародного авторитету. Ці документи — суть неформальної кодифікації, яка здійснюється з метою вироблення найбільш адекватних і юридично досконалих міжнародних правил для їх широкого застосування у практиці міжнародних відносин. До них належать «Принципи міжнародних комерційних контрактів» Міжнародного інституту уніфікації приватного права (УНІДРУА), розроблений Комісією з європейського договірної права Звід положень «Європейське договірне право» і Кодекс інформаційного права Європи «Inforights». Спеціалісти різних країн прогнозують радикальні зміни в галузі міжнародно-правового регулювання інформаційних обмінів та комунікації внаслідок формування єдиної світової комунікаційної системи, тобто глобального «інформаційного поля», що потребує адекватних міжнародно-правових рішень.

У Окінавській хартії глобального інформаційного суспільства³⁰⁴, що є передусім закликом до всіх як у державному, так і приватному секторах ліквідувати міжнародний розрив у галузі інформації знань (п.5 хартії), відзначається: «Приватний сектор відіграє життєво важливу роль у розробці інформаційних та комунікаційних мереж в інформаційному суспільстві. Але завдання створення завбачливої, транспарентної та недискримінаційної політики та нормативної бази, необхідної для інфор-

маційного суспільства, лежить на урядах. Нам необхідно по-турбуватися про відповідність правил, які стосуються інформаційних технологій, докорінних змін в економічних угодах з урахуванням принципів ефективного партнерства між державним та приватним сектором, а також транспарентності та технологічної нейтральності процедури» (п.7). Серед інших рекомендуються такі основні принципи та підходи:

- продовження сприяння розвитку конкуренції та відкриттю ринків для інформаційної технології (ІТ) та телекомунікаційної продукції і послуг разом з недискримінаційним та заснованим на витратах підключенні до основних телекомунікацій;
- захист прав інтелектуальної власності на інформаційній технології має важливе значення для просування нововведень, пов'язаних з ІТ, розвитку конкуренції та широкого впровадження нових технологій;
- розвиток транскордонної електронної торгівлі завдяки сприянню подальшій лібералізації, поліпшенню мереж та відповідних послуг і процедур у контексті жорстких рамок Світової торгівлі організації (СОТ), продовженню роботи у галузі електронної торгівлі у СОТ і на інших міжнародних форумах та застосуванню чинних правил торгівлі СОТ до електронної торгівлі;
- послідовні підходи щодо оподаткування електронної торгівлі, що ґрунтуються на загальних принципах, разом з недискримінацією, рівноправністю, спрощеністю та іншими ключовими елементами, узгодженими у контексті роботи Організації економічного співробітництва і розвитку (ОЕСР);
- продовження практики вивільнення електронних переказів від митних зборів;
- просування ринкових стандартів, включаючи, наприклад, технічні стандарти функціональної сумісності;
- розвиток ефективного та значущого механізму захисту особистого життя споживача, а також захисту особистого життя при обробці даних про особу, забезпечення при цьому вільного потоку інформації, а також подальший розвиток та ефективне функціонування електронної ідентифікації, електронного підпису, криптографії та інших засобів забезпечення безпеки та вірогідності операцій.

Необхідно також (п.8) віднайти ефективні політичні рішення актуальних проблем, як наприклад, намагання несанкціонова-

ного доступу та комп'ютерні віруси. Ми будемо і надалі залучати представників промисловості та інших посередників для захисту важливих інформаційних інфраструктур».

Актуальним є питання і про те, хто є власником інформаційних ресурсів, що становлять СНІР України. Це питання є доречним також і щодо представників індивідуальної форми власності. Державне втручання в економіку нині піддається остракізму. Якщо навіть йтиметься про посилення ролі держави, то це обернеться, в остаточному підсумку, її подальшим самовиведенням з господарської практики, активізацією діяльності з дерегулювання економіки. Аргументами є поширені міркування про неефективність державної власності, про те, що в неї немає господаря, «державне — це нічیه» і т.п. Як свідчить світовий досвід у цілому, державна власність може бути дуже ефективною, коли держава як суб'єкт власності формує адекватний об'єкт власності та відповідний господарський механізм реалізації своїх прав власника³⁰⁵.

Місце органів НТІ, інших організаційних утворень у загальнодержавній системі національних інформаційних ресурсів визначається не тільки організаційними або технологічними факторами. Не менш важливими є проблеми вільного доступу, публічності спеціальної інформації, безплатності вже оплаченої суспільством інформації. У цьому питанні вже спостерігається деяка позитивна конвергенція: центри НТІ намагаються акумулювати фонди документів та обслуговувати індивідуально споживача (що раніше не було їм притаманно), а бібліотеки швидко розвивають нетрадиційні види обслуговування — телекомунікаційні послуги, доставку документів з інших фондів, аналітичну та реферативну роботу³⁰⁶.

Для координації та успішного розвитку вже наявної тенденції необхідно налагодити інвентаризацію інформаційних ресурсів та прагнути єдиного підходу до роботи довідково-пошукового апарату бібліотек та центрів, розробити рекомендації стосовно єдиних форматів, однастайності щодо платності (або безплатності) доступу. За взірць може слугувати Інтернет, коли споживач, керуючись власними інтересами, здійснює пошук за тематикою, адресою, автором тощо, а через який фізичний сервер здійснюється цей пошук — не є важливим. Цей великий принцип прозорості «www» мережі Інтернет набагато доцільні-

ше було б використати для побудови системи національних інформаційних ресурсів, особливо в частині їх формування та поширення.

Багато з цих проблем не розв'язуються досі ще й тому, що не відбулося практичної перебудови на ринкову економіку. Зокрема, формування ЗІР на кооперативних засадах не застосовується за відсутністю стимулів до поєднання та економії фінансових ресурсів. Крім того, широким полем для співробітництва є проблема платності інформації, в тому числі тієї, яка вже оплачена платником податків (Нагадаємо, що вже нині таблиці змістів за тематикою пошуку, в тому числі наукової періодики, анотації статей через Інтернет надаються безоплатно. Плата надається лише за видачу повних текстів). Це також означає переосмислення ролі постачальників реферативної інформації (наприклад, газета «Все — всім»). Суміжним з цим є питання юридичного захисту інформаційних центрів, бібліотечних мереж тощо як державних установ. Якщо до 1991 року функціонували органи, в тому числі на рівні органів місцевого самоврядування, які представляли інтереси держави у цій сфері в цілому, то нині цю функцію покладено на суди. Тому юридична підтримка інформаційної інфраструктури загальнодержавного спрямування в наш час може набути ваги потужного об'єднуючого чинника. Це повною мірою стосується як проблеми Copyright, так і питань повсякденної діяльності.

Розв'язання цих проблем цілком і повністю залежить від їхнього сприйняття на урядовому рівні, від включення їх до інформаційної політики держави. Сьогодні немає державного органу або відповідного рівня громадської організації, яка могла б взяти на себе таку міжвідомчу координацію різноманітних інформаційних мереж. Через непередбачуваність характеру виділення коштів серйозно розраховувати на дієвість координації з боку якогось одного відомства (наприклад, Міністерства освіти і науки) не доводиться. Тому маємо погодитись з непрацездатністю державної структури, заздалегідь передбачаючи її заміну або доповнення в суспільно вагомих функціях приватною структурою. Оскільки, принаймні в Україні, органи НТІ, НТБ не підлягають приватизації, а проблема залишається поза увагою державної інформаційної політики, набувають поширення кооперативні форми, форми асоціацій щодо роботи у згаданому

напрямі (наприклад, Всеукраїнська асоціація інформаційних служб, створена наприкінці 2001 року).

Настав час зосередитися на інституційному інформаційному ресурсі так, як у минулі роки займалися головними галузями матеріального виробництва. Мають бути жорстко визначені склад основних інформаційних завдань суспільства, система пріоритетів у створенні суспільно вагомих змістовних інформаційних ресурсів, потреби громадян та організацій у такій інформації, завдання щодо пристосування інформаційної техніки, уніфікованих процедур та стандартів до вирішення основних інформаційних завдань та задоволення потреб споживачів інформації³⁰⁷.

Викладене підводить до висновку про необхідність розробки і послідовної реалізації державної інституційної інформаційної політики в реальних умовах економічної трансформації України, що охоплює державний і недержавний сектори, оскільки в жодному з них реалізація господарських відносин на засадах новітнього інституту власності не призвела до створення умов сталого розвитку. Це вимагає посилення організаторської функції держави, введення більшої плановірності в процес формування і використання змістовного інформаційного ресурсу, виробничих засад його відтворення на загальнодержавному і регіональному рівнях, формування на нових засадах об'єктів, суб'єктів і господарського механізму реалізації прав власності на інформаційний ресурс та окремі його складові.

Основними заходами щодо становлення цивілізованого інформаційного ринку з урахуванням інноваційної моделі формування ЗІР, розвитку системи національних інформаційних ресурсів можна вважати:

- забезпечення державної підтримки вітчизняної інформаційної інфраструктури шляхом розвитку нормативно-правової бази, яка регулює відносини учасників СНІР та інформаційного ринку стосовно процесів формування, збереження, поширення, розпорядження ЗІР, а також розвитку антимонопольного напрямку законодавства в інформаційній сфері;

- організаційно-фінансове забезпечення матеріальної бази інформаційної сфери державного сектора (інформаційна та телекомунікаційна інфраструктури; галузі промисловості, що забезпечують виробництво засобів обчислювальної техніки та зв'язку з метою формування, функціонування і розвитку СНІР);

- інвентаризація вітчизняних інформаційно-змістовних ресурсів; введення відповідних показників статистичної звітності для відображення формування, поточного стану та результатів використання ЗІР;

- розробка та впровадження загальносистемної (в розумінні СНІР) нормативно-методичної бази, що зумовлено різноманітним складом інформаційних джерел, які утворюють змістовний інформаційний ресурс, у тому числі формування інформаційних масивів за конкретними видами інформаційних джерел;

- здійснення захисту прав власності на інформаційні ресурси, системи, продукти та послуги шляхом нормативного закріплення прав власності у реєстрі державних та інших інформаційних ресурсів і систем; розробка положень (концепції) страхування інформаційних ризиків; ліцензування діяльності з інформаційного міжнародного обміну;

- активне залучення приватного капіталу до розвитку інформаційної сфери, зокрема, процесів відтворення ЗІР у системі національних інформаційних ресурсів за рахунок використання сучасних інформаційних технологій.

Важливою складовою інституційної політики формування і використання інформаційного ресурсу є відстеження використання науково-технічної інформації, до якої, як правило, належить документована інформація, що виникає внаслідок наукової та науково-технічної діяльності. Як зазначалося, з погляду застосування або споживання НТІ вона складається з двох взаємодоповнюючих напрямів: потік, що спрямовується для забезпечення діяльності суто наукового співтовариства, в якому на основі попередніх досягнень генеруються нові знання, ідеї, відкриття, та потік, використання якого є необхідним у період переходу від наукових досягнень до виробництва нової продукції і технологічних процесів, маркетингу, розподілу (впровадження) цієї продукції, її масового виробництва тощо.

- На підставі цього можна помітити, що ринок інформації, зокрема НТІ, має суттєві відмінності, які полягають у тому, що інформація про результати науково-технічних досягнень має соціальний характер і спрямована на забезпечення поінформованості суспільства в цілому; інформація потребує оперативного використання одночасно з її збереженням та цілісністю; вона має здатність породжувати нову інформацію, є відкритою та

інтернаціональною, але потребує захисту від несанкціонованого використання.

З переходом до нових форм господарювання, коли інформаційні продукти та послуги стають основним джерелом життєдіяльності їхніх організацій-виробників, а суспільство вимагає дедалі більшої інформації для забезпечення сталого розвитку, реструктуризація системи НТІ стає однією з найважливіших. Так, саме у секторі НТІ як частині науково-професійної інформації зосереджено 15 — 20% змістовно вагомої інформації, саме стан цього сектору повною мірою визначає ступінь розвитку науки, освіти, культури, соціальної стабільності суспільства³⁰⁸. При цьому як власник державної системи НТІ саме держава, вкладаючи кошти в інформаційну діяльність, має виходити з того, що результати цих вкладень належать також державі, а отже, її громадянам — без будь-якої оплати, оскільки створені за їхній рахунок. Це призводить до того, що безоплатна або пільгова реалізація інформаційних продуктів та послуг, вироблена за рахунок держави, порушує свободу конкуренції і свідомо ставить недержавних учасників інформаційного ринку в гірші умови. Ця проблема також належить до сфери інформаційної політики і потребує координованого розв'язання на рівні держави.

Система наукової і технічної комунікації (каналів розподілу, поширення інформації), що становить підґрунтя СНІР, також значною мірою підпадає під вплив різних чинників, які можна розглядати як зовнішні та внутрішні³⁰⁹.

До зовнішніх чинників належать: економічні, політичні, соціальні та культурні особливості конкретної держави, а також держав, організації яких співробітничать з конкретною інформаційною системою; законодавчі та юридичні фактори; наявність конкурентів, що виробляють аналогічну продукцію, та фірм поширювачів; стан сфери потенційних споживачів (потреба в інформації, платоспроможність тощо), розвиток телекомунікаційних систем передавання інформації. Усі ці чинники перебувають у постійній взаємодії, підпадають під вплив повільних змін (наприклад, політична система) та одночасно є досить динамічними (наприклад, податкове законодавство чи засоби телекомунікації). Усе це породжує комплекс проблем та обме-

жень в організації системи наукової та технічної комунікації або узагальнено — в інформаційній діяльності.

До внутрішніх факторів належать: виробнича та маркетингова діяльність з виробництва та поширення інформаційних продуктів і послуг, взаємовідносини з партнерами, відносини структури, що забезпечує поширення НТІ, з іншими службами установи, позиція на інформаційному ринку (знаність фірми), стратегія ціноутворення, організація рекламної діяльності, можливість швидкого реагування на зміни вимог щодо форми та якості інформаційних продуктів та послуг, технічного оснащення, наявності доступу до телекомунікаційних мереж.

Ці чинники стимулюють систему комунікації до динамічного розвитку, реструктуризації основних компонентів, а також забезпечують сталість системи комунікацій, визначають напрями та необхідні заходи інституційної політики формування і використання інформаційного ресурсу.

У Російській Федерації, наприклад, координація робіт з реструктуризації системи НТІ та визначення принципів функціонування Державної системи НТІ (ДСНТІ) провадиться у межах колегіального напрацювання концептуальних засад функціонування і розвитку системи в сучасних умовах, розробки та впровадження загальносистемної нормативно-методичної бази, що забезпечувала б сумісність роботи її ланок.

Федеральний устрій Росії як держави зумовлює й особливості ДСНТІ, координацію робіт у цій сфері, організацію доступу до державних інформаційних ресурсів³¹⁰.

Завданням сучасного етапу вважається розробка умов взаємодії інформаційних центрів різного рівня та руху інформаційних потоків таким чином, щоб споживач з мінімальними витратами отримав всю необхідну інформацію. Для цього передбачається передусім відрегулювати роботу інформаційних центрів різних рівнів у режимі мережі. Завдання потребує нетрадиційного підходу через те, що мережа низових посередників — відділів НТІ розпалась, а до 1997 року на підприємствах РФ їх налічувалося близько 15 тис. Тому проблема поєднання в межах ДСНТІ потребує насамперед визначення:

— конкретних центрів НТІ — депозитаріїв наукової й технічної інформації по регіонах Росії, які стали б опорними ланками в організації інформаційного обслуговування;

— ВІНІТІ як найбільш впливовий та досвідчений, найпотужніший центр НТІ Росії має взяти на себе функції «навігатора» з інформаційних ресурсів НТІ, а також (разом з Інформрегістром) з ресурсів фактографічного характеру разом з ресурсами Інтернет.

У проведенні робіт зі створення навігаційної системи з державних інформаційних ресурсів ДСНТІ мають брати не останню участь територіальні центри НТІ, які повинні не тільки бути представниками федеральних органів НТІ у регіонах, а й забезпечувати реєстрацію інформаційних ресурсів науки і техніки на місцевому рівні³¹¹.

Слід зазначити, що досі на інформаційному ринку Росії, який активно формується, у федеральних інформаційних служб немає сильних конкурентів, наявність яких могла б позитивно вплинути на ціни інформаційної продукції та послуг на користь споживача і зруйнувати існуючий монополізм у інформаційній сфері. Це саме стосується і стану справ в Україні. Рівень бюджетного фінансування федеральних інформаційних служб РФ також не дозволяє їм значно знижувати ціни на інформаційні продукти та послуги. Надання НТІ з державних ресурсів за запитами споживачів відбувається на умовах, які забезпечують відшкодування витрат інформаційних служб на створення інформаційних продуктів та надання послуг, що обумовлено Положенням про ДСНТІ у частині безприбуткової експлуатації державних ресурсів НТІ.

Але, як зазначалося³¹², відбувся цікавий перерозподіл, своєрідний «перекіс» щодо перерозподілу надходження світового потоку інформаційних ресурсів між центральними закладами інформації та регіональними, а саме у розподілі державних інформаційних ресурсів. У 1990 році з державних асигнувань РФ на науку (140 трлн. руб. у цінах 1997 року) 3,5 трлн. руб. припадало на систему НТІ. Третина цих коштів надходила у центральні інститути та провідні бібліотеки — розпорядники основних інформаційних ресурсів, дві третини йшло на фінансування відділів та служб НТІ на підприємствах та в організаціях (близько 15 тис. служб). У 1997 році наука отримала 11 трлн. руб., а НТІ — 350 млрд. руб. Приблизно 90% всіх коштів НТІ отримали центральні інститути інформації, центри інформації та бібліотеки, розташовані у Москві, Санкт-Петербурзі та Но-

восибірську, і лише десь 10% спрямовано на підтримку відділів та служб НТІ на підприємствах та в організаціях (на 1998 рік у таких службах працювали у середньому три людини). Таким чином, якщо на 1990 рік розподіл державних коштів був таким: 30% — на центр, 70 — на регіони Росії, то на 1998. рік цей розподіл (без Санкт-Петербурга та Новосибірська) становить: 85 — на центр і 15% — на регіони. Те саме стосується і розподілу світового інформаційного потоку: замість 40% (1990 рік) надходить 15% (1998 рік), з них лише 5% припадає на регіони. Крім того, якщо раніше у регіонах існувало 13 базових патентних фондів (не дублів ВПТБ), то у 1998 році немає жодного вагомego патентного фонду в регіонах Росії. Цей стан справ і посприяв значною мірою тому, що мав бути змінений принцип побудови «старої» ДСНТІ: багаторівневий ієрархічний принцип, де інформаційні потоки мали висхідний (доцентровий) і низхідний (відцентровий) характер, кінцевий споживач працював виключно через відділи НТІ, передусім на підприємствах та в установах. Нині ж у центрі «нової» ДСНТІ постає саме споживач, інформаційна інфраструктура набуває вигляду мережі і працює у відповідному режимі. Стає зрозумілим, що такі найважливіші центри, як ВІНІТІ, Інформрегістр, ВНТІЦентр (усі — в Москві) не втрачають своєї ролі, в тому числі й щодо тематики діяльності, а набувають функціональної значущості як своєрідні вузли національної мережі (за аналогією з Інтернет).

Слід також окремо спинитися на сучасній ролі Всеросійського (колишнього Всесоюзного) науково-дослідного інституту міжгалузевої інформації (ВІМІ), створеного у вересні 1968 року як член ДСНТІ³¹³.

ВІМІ завжди був членом ДСНТІ, але мав своє особливе місце та значення у цій державній структурі. Ця особливість полягала в тому, що ВІМІ брав до своєї інформаційної системи документи з інших загальносоюзних інформаційних центрів — генераторів НТІ (ВІНІТІ, ВНТІЦентр та інші), використовував цю інформацію для обслуговування своїх абонентів, але сам не передавав своєї унікальної інформації до ДСНТІ.

Основним завданням новоствореного ВІМІ було визначено відбір та передання народному господарству СРСР науково-технічних досягнень оборонного комплексу, тобто фактично те, що нині дістало завуальовану назву «процес використання по-

двійних технологій». Крім того, на інститут було покладено функції комплексного інформаційного обслуговування розробок (НДДКР)³¹⁴, виробництва та органів управління ВПК, координація видавничої діяльності галузевих інститутів оборонних галузей промисловості, а також роль головного розробника Міжгалузевої автоматизованої системи НТІ (МІАС «Созвездие»). Загальне методологічне керівництво інститутом здійснював Військово-промисловий комітет (комісія) Ради Міністрів СРСР. За активної підтримки всіх своїх дев'яти галузевих інститутів ВПК створив МІАС, яка багато в чому концептуально корелювала з відомою американською системою Agranet (родоводом сучасної мережі Інтернет), хоч і з суттєво різними завданнями. ВІМІ став не тільки формальним, а й реальним лідером НТІ в оборонних галузях промисловості (ОГП), навколо якого сформувалась ієрархічна, багатоланкова Єдина система НТІ ОГП, ядром якої була МІАС «Созвездие». ЄСНТІ ОГП функціонувала на засадах системних угод між її учасниками, що регламентували тематику, номенклатуру, джерела та зони обслуговування кожної її ланки — від ВІМІ до відділів НТІ підприємств, тобто була підсистемою або, точніше, вмонтованою системою у ДСНТІ СРСР. Розпад СРСР зачепив ВІМІ, як і весь ВПК, внаслідок чого розпалась і припинила своє існування ЄСНТІ ОГП та її автоматизоване ядро МІАС «Созвездие» (крім центральної ланки у ВІМІ). Але залишились інформаційні ресурси (тобто ЗІР), у тому числі на підприємствах, в установах та організаціях, що підпорядковувалися тій «дев'ятці», інформаційну ланку якої очолював ВІМІ, які незалежно від форм збереження, містять інформацію, що становить або становила державну таємницю, конфіденційну інформацію ще й дотепер.

Відомо, що впродовж десятиліть у СРСР колосальні кошти вкладалися в оборонний комплекс і тут зосереджувались найкращі «мізки»: йдеться про випускників найкращих вузів країни (Москви, Ленінграда, Києва, Харкова, Мінська, Горького, Свердловська). Для цього ж створювалися й закриті: Арзамас-16, Челябінськ-70 та ін. Було досягнуто визначних успіхів у галузі військових технологій, конкретних видів озброєнь. Усі інформаційні джерела, що дали змогу б використати сьогодні ці досягнення, і дотепер зберігаються на тих самих засадах ЄСНТІ ОГП СРСР у фондах інформаційних центрів та пов'язаних з

ними інформаційних підрозділах підприємств конкретної галузі промисловості РФ.

Звичайно, з боку держави необхідний певний протекціонізм щодо високих технологій. І він успішно розвивається у Росії, яка володіє практично всіма високими технологіями. І їх введення до будь-якої держави, в тому числі й до України, науково-технічний здобуток якої зберігається, принаймні в інформаційному варіанті, в нинішній системі НТІ РФ, може обернутися цілеспрямованими спробами вплинути на технічну та комерційну політику тієї держави, до якої ця технологія ввозиться. Це досить поширене явище в усьому світі, й у переважній більшості країн багато питань у цьому напрямі вирішується в руслі інформаційної політики держави.

У ВГМІ накопичені унікальний досвід міжгалузевого збору та поширення військово-технічної, технологічної, економічної та іншої інформації з широким спектром застосування, включаючи військово-промисловий комплекс, машинобудування, медицину, обчислювальну техніку, інформатику, обробку матеріалів тощо. З цілого ряду російських (у тому числі радянських) та зарубіжних технологій, устаткування та виробництв є бази та банки даних інвестиційних проектів значного обсягу, реалізація яких потребує чималих коштів. З переходом до ринкової економіки, узвичаєнням нових економічних умов, зокрема, й пов'язаних з приватизацією значної частини оборонних виробництв, реалізацією накопиченого та того, що розробляється, технологічного потенціалу на ринкові технології та устаткування, у ВІМІ було створене відділення системних досліджень. На нього були покладені дослідження та інформаційно-аналітична підтримка перелічених завдань, а також пов'язаних з реалізацією новітніх технологій оборонного комплексу.

Безумовно, без належної державної підтримки, створення організаційно-правових, інформаційних та інноваційних механізмів розвитку і використання, включаючи розв'язання проблем інтелектуальної власності, подвійних технологій як у самій РФ, так і за кордоном, технологічний потенціал оборонної промисловості, РАН, Міністерства оборони Росії не може бути ефективно реалізований у найближчому майбутньому³¹⁵.

Одним із заходів для реалізації такої політики держави (і не тільки власне РФ, а й інших зацікавлених країн) є визначення

і забезпечення умов взаємного використання результатів НДДКР з введенням положень, які дали б змогу перейти до економічно та юридично обґрунтованих принципів участі держав (навіть в особі окремих підприємств) у системі використання й обміну такою інформацією.

Як зазначалося, найбільш чутливою сферою інтеграційних процесів військово-технічної співпраці є обмін інформацією, передусім тією, що містить відомості обмеженого доступу та не підлягає відкритому поширенню. Україна здійснює військово-технічне співробітництво з багатьма країнами Східної, Центральної і Західної Європи як членами Європейського Союзу, так і кандидатами в члени ЄС. Чинним законодавством України встановлено (Закон України «Про інформацію», ст.54), що національні інформаційні ресурси в процесі співробітництва з іншими країнами використовуються на основі рівноправного співробітництва. Крім того, відповідно до Закону України «Про державну таємницю» (ст. 32), секретна інформація або її носії можуть бути передані іноземній державі чи міжнародній організації лише на підставі міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, або письмового мотивованого розпорядження Президента України. В Україні діють також і нормативні документи, що регламентують порядок укладання таких договорів³¹⁶.

Однією з перших угод, яка передбачає взаємний захист інформації з обмеженим доступом (таємної і конфіденційної), була угода, укладена Україною з Організацією Північноатлантичного договору в рамках виконання Програми «Партнерство заради миру». Угоди про взаємний захист таємної інформації та її носіїв підписані з Німеччиною, Францією, Туреччиною, Словаччиною та ін. Угоди України з НАТО та зазначеними країнами містять взаємно погоджені термінологію, ступені секретності, порядок передавання, зберігання, використання таємної інформації, її носіїв та взаємного контролю за використанням сторонами взятих на себе зобов'язань. Поряд з цим чинні угоди про взаємний захист таємної інформації та її носіїв не передбачають механізму і порядку компенсації сторонами матеріальних збитків за порушення зобов'язань, передбачених угодами, внаслідок розголошення, втрати або несанкціонованої передачі

іншим країнам отриманої в процесі співробітництва таємної інформації або її носіїв.

Найбільш неврегульованою в правовому плані як на рівні законодавства України, так і на рівні міждержавних договорів, укладених з Україною, є проблема, пов'язана із захистом інформації з обмеженим доступом, що не становить державної таємниці.

Чинні законодавчі та нормативно-правові акти України не створюють цілісної системи захисту інформації з обмеженим доступом, не встановлюють механізму вирішення цих питань у процесі військово-технічного співробітництва з іншими державами. З усіх угод, укладених Україною з іноземними державами, лише Угода про безпеку підписана з НАТО стосовно виконання Програми «Партнерство заради миру», передбачає зобов'язання сторін щодо взаємного захисту конфіденційної інформації.

Важливим аспектом цієї проблеми, як свідчить аналіз угод про військово-технічне співробітництво та про взаємний захист таємної інформації, укладених Україною з іншими країнами, є відсутність в цих міждержавних актах правових норм про взаємний захист прав на об'єкти інтелектуальної власності, припинення їх порушень, відповідні компенсації за використання прав на вказані об'єкти та зобов'язання сторін щодо застосування відповідних санкцій до порушників цих прав.

Недосконалість чинного законодавства України щодо захисту інформації з обмеженим доступом, що не становить державної таємниці, охорони прав на об'єкти інтелектуальної власності, відсутність відповідних зобов'язань сторін в укладених Україною угодах з іншими країнами, спрямованих на розв'язання цих проблем, веде до зловживань та порушень інтересів держави та прав суб'єктів на об'єкти інтелектуальної власності.

З огляду на наведені проблеми з метою забезпечення рівноправного і раціонального використання інформаційних ресурсів у процесі військово-технічного співробітництва було б доцільним у запропонованому проекті Закону України «Про військово-технічне співробітництво в Україні» окремим розділом визначити норми щодо створення механізму захисту інформації з обмеженим доступом, що не становить державної таємниці, та об'єктів інтелектуальної власності.

Для подальшого поглиблення військово-технічної інтеграції і забезпечення рівноправності у використанні інформаційних ресурсів, що є об'єктом інтелектуальної власності, було б доцільним укласти додаткові угоди з урахуванням вимог Угоди про торговельні аспекти прав інтелектуальної власності, що діє в рамках Світової організації торгівлі і встановлює стандарти, процедури і методики їх застосування для захисту об'єктів інтелектуальної власності, а саме: патентів на винаходи; авторських і суміжних прав; товарних знаків; промислових зразків; компонування інтегральних мікросхем; інформації, що не підлягає розголошенню та ін.

Роль держави у розв'язанні проблем регулювання інформаційної діяльності з погляду управління інформаційно-змістовними ресурсами дістала сучасне обґрунтування також у документі, підготовленому XIII директором Європейської комісії у 1996 році. Цей документ є певною мірою орієнтиром для вироблення державної політики в інформаційній сфері. Назва документа: «Зелена книга про доступ та використання інформації державного сектору в інформаційному суспільстві. Деякі міркування для вироблення позиції Європейського Союзу». У документі поставлено 14 запитань, відповіді на які відображають політику держави. Відповіді на ці запитання стосовно Російської Федерації дав О.Б. Антопольський, директор НТЦ «Інформрегістр», член-кореспондент РАІН. Вони згодом стали концептуальною та методологічною основою з регулювання економічних та майнових відносин у галузі інформаційних ресурсів ДСНТІ³¹⁷.

Для мети цього дослідження видається необхідним навести деякі запитання, запропоновані Зеленою книгою³¹⁸, і надати на них відповідь.

— *Що мається на увазі, коли йдеться про інформацію державного сектору?*

Як у РФ, так і в Україні, відповідь на це запитання є однією з найскладніших. Передусім відсутній перелік організацій, відповідальних за формування державних інформаційних ресурсів (ДІР). Як відомо, статистична звітність (на рівні державних показників) за видами інформаційної діяльності у секторі науково-технічної інформації в Україні так і не набула постійного характеру, а відтак будь-які офіційні показники щодо формування ДІР не будуть повними та вірогідними. Зелена книга про-

понує два можливих підходи до визначення ДІР: функціональний, тобто визначення сфер діяльності, закріплених за державою, та інституційний, або перелік організацій, що є державними. В одних країнах до ДІР належить тільки інформація органів державної влади, в інших — офіційна інформація, а ще в інших — включають інформацію державних установ тощо. Україна не визначилась у цьому питанні навіть на рівні законодавчих положень, надто методологічно.

— *Яким має бути рівень оплати (за змістовну інформацію, що надається)?*

Європейські країни прагнуть до встановлення тарифів за принципами:

- необтяжливості для громадян;
- встановлення для приватного сектору рівня прибутку, який би виправдовував вкладення в обробку та вторинне використання інформації;
- створення умов сприяння для приватного сектору;
- відшкодування певної частки видатків державних організацій.

Деякий прогрес визначився в інформаційному обслуговуванні матеріалами ДІР Українського інституту промислової власності (патентний фонд). Але ціни, що зумовлюють патентний пошук (не на предмет надання патенту), також не є тарифікованими, а залежать від складності пошуку, що визначається його виконавцем.

Слід підкреслити, що ці два запитання є ключовими для здійснення державної інформаційної політики, визначення рівня бюджетного фінансування інформаційної діяльності, розробки положень для бухгалтерського обліку та звітності щодо ДІР України, проблем класифікації та реєстрації змістовних інформаційних ресурсів держави.

— *Питання конкуренції та авторського права.*

Проблему авторського права щодо створення ШП та умов надання їх у обіг в Україні нами проаналізовано. Було визначено, що за Законом України «Про науково-технічну інформацію» (ст.2) НТІ є продуктом інтелектуальної творчої праці і становить об'єкт права інтелектуальної власності, в чому, власне, немає ніяких сумнівів. Але чим захищена аналітична праця, яка і є суттю створення інформаційної продукції та послуг (ШП)?

При цьому згідно з цим законом (ст.10, п.3) використання органами та службами НТІ переданих їм підприємствами та організаціями матеріалів і технічної документації провадиться на умовах, встановлених підприємствами й організаціями — власниками інформації. І далі: «...органи і служби НТІ, яким передається така інформація, гарантують захист прав інтелектуальної власності, додержання комерційної таємниці, захист законних інтересів юридичних та фізичних осіб — творців інформації про науково-технічні досягнення». Звичайно, використання документів, наданих «творцями інформації», відбувається за умов додержання щодо них положень авторського права, але продукування аналітичних матеріалів (ст.1, абз.7), їх створення та поширення, що є «основними завданнями національної системи НТІ» (ст.9, абз.4, 5, 7), не захищається жодними конкретними положеннями Закону України «Про авторські і суміжні права», крім положень, що стосуються баз даних.

Виникає також запитання, як забезпечити різноманітні джерела отримання інформації, в тому числі державні та приватні, і при цьому дотримуватися принципів чесної конкуренції. Тут важлива, в аспекті розв'язання цього питання, наявність державних та недержавних ЗМІ, державних (і виключно державних!) органів НТІ та науково-технічних бібліотек, ДІР, що створюються лише в органах влади та адміністративних і відомчих установах інших інформаційних органів, та їх статус.

ДІР завжди створюються під цільові або функціональні завдання, що визначаються нормативними документами або завданнями відповідних відомств, міністерств, органів влади та управління, що формують інформаційну політику в межах держави або окремого відомства чи регіону. Інакше кажучи, вони є, з цього погляду, корпоративними (для забезпечення внутрішніх користувачів, з зовнішнім замовником включно) та масового користування (для забезпечення і внутрішніх, і зовнішніх користувачів однаковою мірою). У більшості організацій та підприємств галузевого підпорядкування ДІР з НТІ формуються для інформаційного забезпечення їх науково-технічної та виробничої (підприємницької) діяльності. Вторинними користувачами можуть бути будь-які суб'єкти інших організацій, підприємств, фірм, приватні особи, зацікавлені в отриманні матеріалів цих ДІР або ІПП. Комерційні інформаційні служби,

що здійснюють обробку ДІР з НТІ та формують нові ІПП за державними замовленнями, спрямовані на тиражування та реалізацію продукції широкому ринковому споживачеві. При цьому принципи формування цін залежать від отримання економічної вигоди і (в міру можливості) рідко узгоджуються з державним замовником, хоч ціни, що встановлюються, мають враховувати частку держбюджетних вкладень (коштів) у створення продукції і забезпечувати зниження цін на неї, а це таким службам зовсім не вигідно. Державні замовники задовольняються отриманням особистого безплатного обслуговування цими ІПП.

Тому відповідь на це запитання залежить від створення механізмів ефективного державного регулювання суспільно-виробничих відносин у сфері ДІР з НТІ.

Нині це питання перебуває у стані загальної невизначеності, а окремі його рішення є надто заполітизованими.

— Чи потрібна універсальна служба інформації державного сектору?

Ця ідея була висловлена експертами Євросоюзу і відтоді обговорюється у багатьох країнах Європи. Природно, що значною мірою вирішення такого питання залежатиме від загального політико-адміністративного устрою конкретної держави, соціально-економічної політики, яку провадить її уряд. Досить детально питання щодо НТІ та видів інформаційних джерел, які можна кваліфікувати як НТІ, було висвітлене у п. 1.2. Тут можна лише додати, що на даний час в Україні, та, за нашими даними, і в інших країнах СНД, відсутні економічні нормативи функціонування державних безприбуткових інформаційних служб, до яких може бути віднесена система органів НТІ в цілому, відомчі інформаційні служби, науково-технічні бібліотеки. У будь-якому разі варіант реєстрації прав на ресурси як об'єкт інтелектуальної власності в межах українського законодавства не опрацьований. Останнім часом у юридичній та спеціальній літературі згадується змішаний варіант, коли ДІР перебуває одночасно й у речовій, і в інтелектуальній власності. Але й тут питання про реєстрацію прав власності також залишається відкритим. У будь-якому разі видається необхідним визначення сфери повноважень передусім щодо органу, який здійснює державну реєстрацію ДІР, а тим самим і обумовити сферу ефективності його використання і для досягнення інших цілей. Крім того, слід бра-

ти до уваги і «чорний інформаційний ринок», який на 100% використовує державний інформаційний ресурс. Реальна інформаційна та економічна політика, безумовно, має враховувати і цей чинник поряд з тим, що значна частина ДІР не має платоспроможного попиту і тому не є рентабельною. Ще одним чинником є питання захисту ДІР від руйнування та несанкціонованого використання, зокрема, при наданні його в Інтернет. Йдеться про створення організації, яка мала б монополне право на ДІР в Інтернеті та забезпечувала б доступ до них масового користувача.

Відповіді на ці запитання свідчать, що політика продукування змістовних інформаційних ресурсів країни має зважати на основні напрями інформаційної політики Євросоюзу, повноправним членом якого має стати й Україна, на рекомендації Ради Європи.

Тільки на основі виваженої державної економічної та інформаційної політики, що реалізується науково і політично обґрунтованими правовими нормами законів та підзаконних актів, які відповідають Конституції України, можна забезпечити раціональне використання наукових здобутків, новітніх технологічних рішень, ноу-хау тощо для економічного і соціального розвитку країни та сталого функціонування системи національної безпеки. Це також сприятиме рівноправному використанню ЗІР за результатом науково-технічної діяльності в процесі міжнародного співробітництва та розвитку інтеграційних процесів.

Варто підкреслити, що, незважаючи на понад десятилітній проміжок часу, політика з використання ЦНТІ в галузі промислової та бізнес-інформації на відміну від наукової та науково-технічної ще перебуває у стадії формування. Але вже тепер стає очевидним, що, по-перше, доки науці не буде приділена належна увага і відповідно не зросте потреба у НТІ, бізнес-інформація не посяде провідного місця в діяльності центрів та в системі НТІ в цілому. По-друге, якщо й відбудеться, центри вже не відмовляться повністю від бізнес-інформації, бо одночасне володіння як науковою, так і комерційною інформацією дасть змогу їм відігравати набагато суттєвішу роль у кооперації науки з виробництвом, ніж це відбувалося раніше.

Стан економічного розвитку України на сучасному етапі потребує докорінної зміни орієнтирів розвитку, оскільки при кон-

сервації існуючого погляду на інституційну політику формування і використання національного інформаційного ресурсу Україна може зайняти постійне місце на периферії розвитку. Без зміни погляду на державну інформаційну політику відпрацювання інноваційно-інвестиційної моделі розвитку дуже ускладнюється.

Розвиток інституції формування і використання змістовного інформаційного ресурсу визначає напрям розвитку соціально-економічної системи, а тому розуміння розвитку цієї інституції сприяє розумінню розвитку та механізмів управління системою національних інформаційних ресурсів України.

3.1.1. Інформаційна безпека держави та основні елементи її забезпечення

Підґрунтям поняття «інформаційна безпека» є поняття «безпека». Це стан захищеності важливих інтересів особистості, суспільства, держави. Життєво важливі інтереси можна визначити як сукупність потреб, задоволення яких забезпечує існування та можливості прогресивного розвитку особистості, суспільства, держави, а загрозу безпеці — як сукупність умов та факторів, що створюють небезпеку життєво важливим інтересам. Тоді захист національної безпеки можна розглядати як державну політику та систему заходів економічного, політичного, організаційного та іншого спрямування, адекватних загрозам життєво важливим інтересам особистості, суспільства і держави і спрямованих на виявлення і запобігання таким загрозам³¹⁸.

До життєво важливих інтересів держави передусім належать ті, що ґрунтуються на принципах сильної держави, територіальної цілісності, незалежності, суверенітету. Під інформаційною безпекою, як правило, розуміють стан захищеності життєво важливих інтересів особистості, суспільства, держави в інформаційній сфері (середовищі), де інформаційне середовище — це сфера діяльності суб'єктів, пов'язана зі створенням, перетворенням та споживанням інформації.

Основні загрози інформаційній безпеці в інформаційній сфері утворюються за умов:

— загрози від впливу недоброякісної інформації (недостовірної, хибної, дезінформації) на життєво важливі інтереси особистості, суспільства, держави;

— загрози життєво важливим інтересам особистості, суспільства, держави у зв'язку з неправомірним впливом на виробництво інформації і неправомочним доступом до інформаційних ресурсів, систем їхнього формування та використання.

У сучасних умовах дістали значне поширення нові виклики і загрози, пов'язані з інтенсифікацією комунікаційних процесів, широким використанням комп'ютерних технологій, що створило принципово нові канали впливу на соціально-політичний та економічний розвиток суспільства. Слушні в цьому плані висновки³²⁰ про те, що з появою Інтернету виникло нове, універсальне інтерактивне середовище як важливий елемент сучасної політичної системи демократичного типу, що підвищення рівня оперативності обміну інформацією, «прозорості» і доступності останньої, унікальна можливість генерувати інформаційні потоки в обхід державних структур, що всі ці та інші особливості Інтернету тлумачаться у вітчизняній політичній науці як важливі передумови демократизації посттоталітарних систем. Водночас автор зазначає, що в процесі побудови теоретичних моделей нового суспільства нерідко відтісняються на другий план питання безпеки, якісно нові виклики і загрози, ігнорування яких може породити цілий спектр дестабілізуючих ускладнень аж до виникнення рецидивів тоталітаризму.

Запобігання та ліквідація загроз інформаційній безпеці особистості, суспільства, держави ґрунтуються на розробці та реалізації комплексу засобів та механізмів захисту. До них належать організаційні, технічні, програмні, соціальні, правові та інші механізми, що забезпечують локалізацію та запобігання таким загрозам.

Одним із найпотужніших засобів захисту життєво важливих інтересів особи, суспільства, держави в інформаційній сфері є правовий захист. Основний механізм такого захисту реалізується через чотири групи правових норм: норми, що закріплюють права і свободи; норми, що обмежують права і свободи на законній підставі; норми, що диктують та зобов'язують, у тому числі забезпечувати реалізацію прав і свобод; норми про відповідальність за допущені порушення.

Правовий захист інформаційних ресурсів, права на інформацію, свободу інформаційної діяльності та доцільне обмеження цих прав і свобод в інтересах національної безпеки мають

бути реалізовані в межах нової галузі законодавства України — інформаційного. А це потребує реформування чинного законодавства у сфері суспільних інформаційних відносин відповідно до концептуальних і стратегічних засад, схвально сприйнятих у державних органах і серед наукової громадськості³²¹. На сьогодні розв'язання проблем захисту інформації як складової інформаційної безпеки здійснюється фрагментарно і безсистемно на основі ситуаційно обумовлених державних рішень.

У Російській Федерації свого часу був створений Комітет при Президентові Російської Федерації з реалізації Програми формування і розвитку інформаційного законодавства³²², яка містить засади розробки правового забезпечення інформаційної безпеки.

За цією програмою інформаційне законодавство РФ поділяється на п'ять основних складових (що утворюють цю галузь законодавства): про виробництво та поширення інформації; про інформаційні ресурси, продукти і послуги; про виробництво та застосування інформаційних технологій; про захист інформації (інформаційних ресурсів); про відповідальність за порушення, допущені в цій сфері.

За своєю суттю інформаційне законодавство є правовим забезпеченням інформаційної безпеки як діяльності, спрямованої на захист життєво важливих інтересів особистості, суспільства, держави, яке регулюється надзвичайно широким колом окремих норм та спеціальних нормативних правових актів, вже не кажучи про врегулювання питань міжнародної інтеграції телекомунікацій, комп'ютерних мереж, сховищ інформаційних ресурсів та користувачів. Сюди ж долучаються питання про визначення механізмів широкого застосування та впровадження орієнтованих на кінцевого споживача методів і режимів роботи на засадах міжнародних стандартів, а також питання поєднання відкритості та конфіденційності функціонування національної інформаційної інфраструктури.

Взаємодії людини з довкіллям за своєю суттю є інформаційними. Як і будь-які інші, інформаційні відносини мають цивілізовано реалізовуватися на основі врегулювання інформаційних прав та обов'язків суб'єктів інформаційної діяльності, до яких належать особа, суспільство, держава³²³.

Можна тільки констатувати, що в Україні є досить розвинутим правове підґрунтя для діяльності та розвитку системи забезпечення інформаційної безпеки України, більшість правових норм якого відповідають міжнародним стандартам, принципам і нормам забезпечення прав громадян на свободу слова, отримання та поширення інформації. Водночас законодавчі та нормативні акти, що регулюють відносини в інформаційній сфері, потребують удосконалення з метою усунення суперечностей, заповнення прогалин у законодавстві, особливо з питань інформаційної безпеки держави та захисту інформації з обмеженим доступом, що не становить державної таємниці.

Сучасні умови політичного і соціально-економічного розвитку України характеризуються наявністю об'єктивних суперечностей між потребами суспільства в розширенні вільного обміну інформацією та необхідністю збереження окремих обмежень на її поширення. Основою згаданих суперечностей слугують, з одного боку, неможливість розв'язання найбільш актуальних економічних, екологічних, науково-технічних, соціальних та інших проблем суспільства без надання вільного доступу фахівцям, посадовим особам, громадянам та їх об'єднанням до великих масивів відповідної інформації, а з іншого — висока ймовірність заподіяння шкоди природним та законним інтересам держави, підприємства, громадян та інших суб'єктів права за умови повної свободи доступу до згаданих масивів.

Раціональним з погляду сучасних реалій суспільства видається вирішення даної суперечності шляхом створення правових механізмів захисту критичних масивів інформації, баз даних або конкретних відомостей уведенням відповідних категорій таємниць, а саме: крім державної таємниці, також службової таємниці, таємниці особистого життя та конфіденційності персональних даних, комерційної, банківської, професійної таємниць тощо.

Необхідно підкреслити, що колишня фактично монопольна власність держави на інформаційні ресурси та державна і службова таємниці базувалися на єдиній державній формі власності.

У сучасних умовах розбудови державності мало просто визнати актуальність розробки відповідних законів щодо регулювання відносин, пов'язаних із великим різноманіттям таємниць та конфіденційної інформації. Необхідно врахувати і наявність жорстких часових термінів для введення їх у дію. Головна при-

чина цієї специфічної особливості сучасної України є очевидною: правові акти з питань таємниць створюються практично заново.

Державна система захисту інформації, що діяла у колишньому СРСР, повною мірою відповідала визначеним соціально-політичним, соціально-економічним та правовим реаліям.

До них передусім належали:

- фактично монопольна власність держави на інформаційні ресурси країни;
- сувора централізація міжнародного обміну інформацією;
- адміністративно-репресивний характер управління системою захисту інформації;
- можливість обмеження правових засад захисту інформації переважно підзаконними актами;
- просторово-часова локалізація можливих загроз інформації, що перебувала під захистом.

Перераховані ознаки свідчать про несумісність правових засад захисту інформації, що існували раніше, з умовами нормального функціонування правової держави та відкритого суспільства з різноманітними формами власності.

Більш того, вся передісторія захисту інформації у Росії (до 1917 року), а значить, і в Україні сформувала цілком визначений «інформаційний менталітет» громадян, що є зовсім несумісним з інформаційною культурою сучасного суспільства. Як наслідок, численні ситуації, що вирішуються у країнах з розвинутою ринковою економікою за допомогою традиційних, що склалися десятиліттями, механізмів, сьогодні в нас потребують правового регулювання³²⁴.

Відображенням цього факту є дедалі зростаюча кількість законів України, які тією чи іншою мірою стосуються проблеми таємниць та конфіденційності інформації. Насамперед слід назвати такі законодавчі документи, як: Конституція України (прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року); Концепція (основи державної політики) національної безпеки України, схвалена постановою Верховної Ради України 16 січня 1997 року; закони України: «Про інформацію», «Про державну таємницю», Цивільний кодекс України, «Про банки і банківську діяльність», «Про підприємства в Україні», «Про адвокатуру», «Основи законодавства України про охорону здоров'я»,

Кримінальний кодекс України та ін. Кожний з цих актів, спрямований на вимогу задоволення практичних потреб нашого суспільства, містить конкретні умови та критерії роботи з інформацією, доступ до якої має бути обмеженим. Визначаються також і різні види таємниць.

Виокремлення конкретного виду таємниці передбачає і розробку пов'язаної з ним специфічної системи правових відносин, які здійснюються такими способами:

- відповідно до суб'єкта права, інтереси якого порушуються в разі незбереження таємниці (витоку відомостей, що захищаються), наприклад, державна таємниця, особиста таємниця тощо;

- відповідно до фізичних принципів обігу інформації — таємниця листування тощо;

- відповідно до предметної сфери відомостей, що становить таємницю, — комерційна таємниця, професійна таємниця тощо;

- ⁻¹ залежно від суб'єкта права, що дістав доступ до таємниці (відомостей, що її становлять) встановленим чином, — в обов'язковому порядку, якщо це передбачено законодавством, або за дозволом власника інформаційних ресурсів, що містять таємницю, — банківська таємниця, таємниця нотаріату, лікарська таємниця тощо.

Загальними для вказаних видів ознаками у свою чергу є:

- цінність відомостей, що становлять таємницю, в силу неопізнаності з ними третіх осіб;

- наявність правових обмежень, накладених на поширення даних відомостей;

- реалізація власником відомостей, що становлять таємницю, право на їх захист.

Реальні потреби суспільства, насамперед потреби практики державного управління вже нині однозначно свідчать про необхідність розширення сфери правового регулювання питань, що стосуються віднесення конкретних відомостей до будь-якого виду таємниць, причому норми чинного законодавства виявляються тут недостатніми. Важливим свідченням цього є затвердження постановою Кабінету Міністрів України Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які

містять конфіденційну інформацію, що є власністю держави, від 27 листопада 1998 року за № 1893³²⁵. Цей нормативний документ був розроблений та введений у дію у зв'язку з численними небажаними випадками витоку інформації, аби запобігти цьому. При цьому розголошені відомості не мали правових підстав бути кваліфіковані як такі, що належать до державної таємниці.

Водночас слід зауважити, що цією постановою уряду було запропоновано (п.2) міністерствам, іншим центральним органам виконавчої влади, Раді міністрів Автономної Республіки Крим, обласним, Київській та Севастопольській міським державним адміністраціям у межах їхніх повноважень у шестимісячний термін розробити і ввести в дію переліки конфіденційної інформації, що є власністю держави. Тобто цим нормативним актом створено передумови для протизаконного обмеження прав на інформацію, а також її витоку і розголошення. Без визначення на законодавчому рівні правового режиму кожного виду інформації з обмеженим доступом, юридичного розмежування понять «інші передбачені законодавством таємниці» та «конфіденційна інформація», а також без окреслення кола відомостей, які можуть бути віднесені та які забороняється відносити до конкретних видів інформації з обмеженим доступом, встановлення обмежень доступу на рівні підзаконного акта суперечить як Конституції України, так і стандартам Європейського Союзу.

У РФ на основі затвердженого на державному рівні переліку конфіденційної інформації зроблено ще один крок у цьому напрямі і прийнято Положення про порядок роботи зі службовою інформацією обмеженого користування у федеральних органах виконавчої влади³²⁶. У ньому, зокрема, під службовою таємницею розуміють «відомості, що захищаються і не є державною таємницею, несанкціоноване поширення яких державним службовцем, кому ці відомості були доведені у зв'язку з виконанням ним посадових обов'язків, може завдати шкоди органам державної влади, державним підприємствам, установам, організаціям або порушити їх функціонування». Таке визначення прямо свідчить про те, що шкода від несанкціонованого доступу до інформації не обов'язково може мати виключно вартісний (комерційний) характер.

Важливо також зазначити, що в чинному національному законодавстві недостатньо розроблено відомий принцип, за яким сукупність відомостей (або результат їх опрацювання) може потребувати більш серйозного захисту, ніж кожна з відомостей, що складають цей результат. Особливо це помітно на прикладі науково-технічної інформації, де явно простежується ймовірність повільного «нарощування» таємниці, коли цілком ординарна розробка може стати виключним за прибутковістю патентом або новим видом озброєння та ін.

Обговорюючи проблеми інтелектуальної власності, доходимо висновку, що об'єктом права власності слід вважати продукт інтелектуальної діяльності Людини. По суті, це інформація, яка (при її сприйманні) нерозривно пов'язана з матеріальним носієм: це — мозок людини або відчужені від людини матеріальні носії, такі як книжка, дискета чи інший вид «пам'яті» (запам'ятовуючий пристрій)³²⁷. Якщо не брати до уваги філософську дефініцію інформації (як абстрактну субстанцію, що існує сама собою), збереження та передавання інформації без матеріального носія неможливі. Іншими словами, незважаючи на ряд особливостей, інформація разом з традиційними матеріальними об'єктами може і повинна розглядатися законом як об'єкт права власності, з урахуванням організаційних заходів та технічних засобів його захисту.

Інформація як об'єкт власності конкретного власника може фіксуватися залежно від виду інформації у державних (можливо, у приватних) реєстрах, кадастрах тощо, як наприклад, патентний фонд, фонд алгоритмів та програм тощо. Особливості захисту інформації виникають при її збереженні та обробці засобами обчислювальної техніки, у тому числі в автоматизованих системах, які полягають у перенесенні акценту на програмно-апаратні, тобто захист права власності — це додержання:

- конфіденційності інформації — властивості інформаційної технології (ІТ) забезпечувати розкриття інформації лише згідно з правилами обмеження доступу (право розпорядження);

- цілісності інформації — властивості ІТ забезпечувати надання права модифікації (ліквідації) інформації лише згідно з правилами розмежування доступу, а також забезпечувати незмінність інформації в умовах випадкових помилок або стихійного лиха (право володіння);

- доступності інформації — властивості ІТ забезпечувати вільний доступ до інформації в міру виникнення такої необхідності (право користування).

Порушення конфіденційності, цілісності, доступності — це, власне, небезпечні наслідки, зрозумілі власнику (неспеціалістові з обчислювальної техніки), що обговорюються у технічному завданні на ІТ.

Небезпечні наслідки виникають через:

- навмисну діяльність людини, що пов'язана з пасивною взаємодією з ІТ (сприймання випромінювання), яке призводить до порушення конфіденційності;

- навмисну діяльність людини, пов'язану з активним впливом на ІТ (вплив за допомогою штатних засобів на інформацію, на методи її захисту та обробки і засоби, що їх реалізують) без її руйнування, яке призводить до порушення конфіденційності, цілісності щодо модифікації (ліквідації) і доступності;

- навмисну діяльність людини, пов'язану з руйнуванням ІТ, але не з будь-яким, а лише з таким, що призводить до порушення правомочностей власника інформації (але не власника ІТ);

- непередбачувану випадкову діяльність людини та інші причини (помилки устаткування, оператора, програмного забезпечення, стихійні лиха), які призводять до порушення правомочностей власника інформації.

Зазначені види загроз узагальнено охоплюють усі відомі напрями чи канали, за якими здійснюється захист інформації (ЗІР), а точніше захист прав власності на інформацію.

Перші два типи загроз стосуються проблеми несанкціонованого доступу в широкому розумінні, тобто пов'язані з порушенням правил розмежування доступу, прийнятих у конкретній ІТ. Другий тип загроз — це проблема несанкціонованого доступу у вузькому розумінні, тобто порушення правил розмежування доступу тільки за допомогою штатних засобів ІТ: проблема — це проблема фізичної охорони ІТ (замки, стіни, стелі, стійкість до іонізуючих випромінювань тощо). Четвертий вид загроз стосується проблеми захисту прав власності на інформацію в умовах, коли ця проблема допускає досить сувору ймовірнісну оцінку.

Таким чином, захист прав власності на інформацію корелюється з відомими напрямками діяльності, методами та засобами захисту, а безпека інформації — це більш загальна проблема, яка включає, окрім захисту прав на інформацію, захист інших прав власності громадян, які можуть бути порушені через те або інше використання інформації. Окремою проблемою стає і проблема захисту прав власності на ІТ, оскільки устаткування є самостійним об'єктом захисту.

Необхідність комплексного і системного підходу до питань захисту інформації зумовлена тим, що:

- існує значний обсяг відомостей, які не можна повною мірою віднести до державної таємниці або інших законодавчо обумовлених видів таємниць, збереження яких від несанкціонованого доступу є необхідним впродовж обмеженого часу;

- відсутня правова база захисту прав на службову інформацію, що невідступно-зумовлює невинуватене розширення посадовими особами обсягу відомостей, що можуть становити інформацію з обмеженим доступом;

- потребують закріплення основні правові принципи, вимоги і норми захисту конфіденційної інформації.

Взагалі, розробляючи спеціальний правовий акт щодо таємниці такої інформації, доцільно вирішити найбільш актуальну проблему й обмежити сферу його дії в державному сегменті.

Звичайно, це не є перешкодою для подальшого застосування даного правового акта як методологічної основи для інших законів, що стосуються проблем виявлення і запобігання можливим витокам інформації, проблем інформаційної безпеки держави в цілому.

Концепція (основи державної політики) національної безпеки України визначає сім сфер національної безпеки: політичну, економічну, соціальну, воєнну, екологічну, науково-технологічну та інформаційну. Отже, інформаційна безпека є складовою національної безпеки. У концепції досить системно формулюються основні функції, які має виконувати система забезпечення національної безпеки в усіх зазначених сферах. Їх конкретизація (з урахуванням особливостей інформаційної сфери) дає можливість визначити основні функції системи забезпечення інформаційної безпеки України. Але при загальному зростанні кількості законів, що приймаються, поки що залишається ба-

гато таких сфер життя суспільства і громадян, які ще не врегульовані на законодавчому рівні, що дає простір відомчій правотворчості. Національний банк, Державна податкова адміністрація, Державна митна служба, Фонд держмайна, інші центральні та місцеві органи виконавчої влади буквально «наплоджують» нормативні правові акти, до яких самі ж з не меншою швидкістю вносять зміни та доповнення.

Окрім причин загального характеру — необхідність зміцнення правових та демократичних основ держави, підвищення рівня законності, правової культури тощо, необхідність упорядкування, у тому числі й питань, що розглядаються, диктується ще й сучасним станом вітчизняного законодавства: ніколи раніше воно не було настільки складним і до певної міри заплутаним. Це явище у свою чергу має певні причини: у житті нашого суспільства з'явилися якісно нові суспільні зв'язки та відносини, що потребують регулювання «з нуля». До деяких відносин все ще застосовуються норми колишнього союзного законодавства, формально невідкинуті, але вже фактично застарілі й потребують оновлення.

Аналіз чинних нормативно-правових актів дає можливість сформулювати основні функції системи забезпечення інформаційної безпеки України. Створення та забезпечення діяльності державних органів як складових системи забезпечення інформаційної безпеки, по-перше, потребує створення правових засад для побудови її організаційної структури, розвитку та функціонування її окремих елементів, з визначенням та раціональним розподілом функцій, по-друге, кадрового, фінансового, матеріального, технічного та інформаційного забезпечення діяльності елементів системи.

Управління діяльністю системи зумовлює необхідність вироблення стратегії й планування конкретних заходів щодо забезпечення інформаційної безпеки; вимагає постійної оцінки результативності дій, витрат на проведення заходів.

Можна передбачити, що здійснення планової та оперативної діяльності щодо забезпечення інформаційної безпеки охоплюватиме:

- визначення національних інтересів та їх пріоритетів у інформаційній сфері;
- розробку нормативно-правової бази, що регулює інформаци-

ційні 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 спільне розв'язання проблем інформаційної безпеки;

- участь у роботі керівних, виконавчих та забезпечуючих підрозділів цих структур (організацій), спільне проведення планових та оперативних заходів;

- прогнозування, виявлення та оцінку можливих загроз, дестабілізуючих чинників та конфліктів у інформаційній сфері, причин їх виникнення, а також наслідків їх прояву;

- запобігання та усунення впливу загроз та дестабілізуючих чинників на національні інтереси в інформаційній сфері;

- локалізацію, деескалацію та розв'язання інформаційних конфліктів;

- ліквідацію наслідків інформаційних конфліктів або впливу на інформаційні ресурси дестабілізуючих чинників.

3.1.2. Основні елементи системи забезпечення інформаційної безпеки України у сфері науково-технічної діяльності

Світова практика свідчить про те, що кожна держава вживає певних заходів для забезпечення захисту національних інтересів у сфері науково-технічної інформації. Відносини у сфері науково-технічної інформації, пов'язаної із національною безпекою й обороною, регулюються у Великій Британії, Іспанії, Канаді, Німеччині, Швеції та багатьох інших країнах.

Так, у США до категорії інформації, що підлягає засекречуванню, віднесено наукові, технологічні й економічні питання стосовно сфери національної безпеки³²⁸. У Російській Федерації державною таємницею відповідним законом визначено відомості про досягнення науки і техніки, науково-дослідні, дослідно-конструкторські, проектні роботи і технології, що мають важливе оборонне й економічне значення і впливають на безпеку держави³²⁹. У Китайській Народній Республіці державна таємниця включає секретні відомості про народне господарство, соціальний розвиток та про науку і техніку³³⁰.

В Україні законодавча база регулювання суспільних інформаційних відносин щодо державної таємниці створювалася з урахуванням світового досвіду. В преамбулі до Закону України «Про державну таємницю» визначено, що цей закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України.

У цьому законі у статті, яка має назву «Інформація, що може бути віднесена до державної таємниці», встановлено, що до державної таємниці належить інформація у сферах: оборони (п.1), економіки, науки і техніки (п.2), зовнішніх відносин (п.3), державної безпеки та охорони правопорядку (п.4)³³¹.

У частині, що стосується науково-технічної інформації, встановлено, що до державної таємниці належить така інформація: про наукові, науково-дослідні, дослідно-конструкторські та проектні роботи, на базі яких можуть бути створені прогресивні технології, нові види виробництва продукції та технологічних процесів, що мають важливе економічне чи оборонне значення або суттєво впливають на зовнішньоекономічну діяльність та національну безпеку України; про військове, науково-технічне та інше співробітництво України з іноземними державами, якщо розголошення відомостей про це завдасть шкоди національній безпеці України³³².

Отже, використання інституту державної таємниці із захисту національних інтересів у сфері науково-технічної інформації — це світова практика, зумовлена необхідністю національної безпеки. Захист життєво важливої інформації у сферах оборони, економіки, науки і техніки, зовнішньо — і внутрішньополітичної діяльності країн як державну функцію системного і комплексного вирішення цих питань, як правило, відносять до періоду утворення суверенних держав, формування органів державного управління, розвитку міжнародних зв'язків.

Практика свідчить, що правова система державної таємниці — • визнаний усіма країнами інститут регулювання суспільних інформаційних відносин. Державна секретність у різних формах, способах і методах застосування є в усіх розвинутих демократичних країнах світу. Це суверенне право кожної незалежної держави. Водночас слід зауважити, що у світового

співтовариства існують і певні міжнародно-правові обмеження та вимоги щодо створення і функціонування національних систем захисту таємниць.

Законодавство визначає лише основні вимоги до порядку віднесення відомостей у сфері науки до державної таємниці та їх засекречування. Для реалізації цих вимог доцільне вдосконалення механізмів засекречування в науці, особливо фундаментальних досліджень у зв'язку з великою невизначеністю їх кінцевих результатів, багатофункціональністю і багатоваріантністю практичного застосування.

Незважаючи на те, що наприкінці минулого століття геополітична ситуація змінилася, деякі загрози національній безпеці зникли, однак виникли нові, не менш небезпечні, що й передбачає певну орієнтацію державної політики до засекречування результатів фундаментальних і прикладних досліджень.

Відповідно до ступеня секретності інформації та грифів секретності матеріальних носіїв такої інформації, згідно зі світовою практикою, встановлюються єдині вимоги до виготовлення, обліку, користування, зберігання, схоронності, передавання та транспортування секретних матеріальних носіїв інформації. Іншими словами, ступінь секретності інформації та відповідний йому гриф секретності диктують усім суб'єктам порядок поводження з матеріальними носіями інформації з обмеженим доступом. Законом встановлено, що вимоги до поводження із засекреченою інформацією та її матеріальними носіями встановлюються Кабінетом Міністрів України³³³.

У процесі міжнародного співробітництва інформація, що містить державну таємницю і отримана від інших держав, засекречується відповідно до вимог національного законодавства. Інакше кажучи, обмеження доступу до такої інформації встановлюється відповідно до узгоджених ступенів секретності носіїв інформації, що передається (отримується) сторонами в процесі такого співробітництва. Регламентує це, як зазначалося, і Закон України «Про державну таємницю» (ст. 3). При цьому нагадаємо, що це передбачається у випадках, коли національні законодавства сторін містять різні вимоги до порядку обмеження доступу до інформації, що охороняється відповідно до світової практики і нормативних вимог, чинних в Україні, і якщо взаєм-

но узгоджені критерії і правила у вигляді зобов'язань сторін, що викладаються в окремій угоді (договорі).

Наведені вимоги є обов'язковими і в процесі міжнародного співробітництва у галузі наукової та науково-технічної діяльності з використанням інформації, що становить державну таємницю.

Загальновизнаним у світовій практиці є принцип відкритості інформації, дотримання права на інформацію і свободу інформаційної діяльності та гарантування права власності на інформацію. Обмеження доступу до інформації (віднесення до категорії з обмеженим доступом, засекречування, встановлення конфіденційності) є винятком із загального принципу відкритості інформації і здійснюється тільки на підставі законодавства.

У демократичному суспільстві обмеження права власності на інформацію або припинення цього права здійснюється, як правило, на договірних засадах укладанням відповідного договору між уповноваженим державою органом і власником інформації. Примусове відчуження інформації або її матеріальних носіїв може бути застосоване, як це передбачено Законом України «Про державну таємницю», лише в інтересах національної безпеки України у випадках, «якщо власник секретної інформації або її матеріальних носіїв відмовляється від укладання договору або порушує його, за рішенням суду ця інформація або її матеріальні носії можуть бути вилучені у власність держави за умови попереднього і повного відшкодування власникові їх вартості»³³⁴. Стосовно державної таємниці суспільна необхідність полягатиме в тому, що розголошення таких відомостей «може завдати шкоди національній безпеці України»³³⁵.

Аналіз правових аспектів практичного застосування закону щодо випадків примусового відчуження й усупільнення іншої інформації з обмеженим доступом, що не становить державної таємниці, з мотивів національної безпеки та іншої суспільної необхідності свідчить про те, що правові механізми вирішення цих питань у державі поки що відсутні. З цих причин в Україні склалася ситуація, коли вітчизняні наукові здобутки, новітні технологічні рішення, ноу-хау тощо, які містять відомості з обмеженим доступом, що не становлять державної таємниці, і які безпосередньо пов'язані з національною безпекою та про-

гресивним економічним і соціальним розвитком, можуть бути використані тільки на договірній основі. Іншими словами, використання з метою суспільної необхідності новітніх знань і технологій в окреслених випадках у зв'язку з відсутністю ефективно діючих правових механізмів реалізації закону захисту інформації (примусового відчуження та усупільнення інформації) залежатиме не від підстав і порядку, встановленого в державі, а від волі й бажання дослідника, розробника і виробника. А це може мати тяжкі негативні наслідки.

Принцип захисту інформації — це науково обґрунтовані положення, правила, рекомендації щодо норм поведінки та практичної діяльності у сфері забезпечення функціонування системи захисту інформації. При цьому принцип на відміну від закону захисту інформації не тільки відображає об'єктивно існуючі в суспільстві зв'язки процесів і явищ, а й орієнтує, на певні дії в конкретних умовах, спрямовані на досягнення визначених цілей, що дає змогу:

- забезпечити баланс інтересів особи, суспільства, держави;
- всебічно враховувати доцільність віднесення відомостей до державної таємниці, виходячи з можливих позитивних і негативних наслідків цього акту;
- забезпечити обіг відомостей, віднесених до державної таємниці, в умовах, своєчасно обмежених режимними заходами;
- витрачати кошти державного бюджету на захист тільки відомостей, розголошення яких дійсно завдасть шкоди життєво важливим національним інтересам.

Доповнення чинного законодавства такими нормами слугуватиме правовою базою для розробки відповідних нормативних документів, спрямованих на забезпечення реалізації цих принципів у практичній діяльності всіх суб'єктів України, що мають відношення до сфери, пов'язаної з державною таємницею.

Ми вже зазначали, що українська система віднесення відомостей до державної таємниці є досить ґрунтовною, дає змогу враховувати в широкому плані шкоду державі, однак ця система в нових умовах господарювання потребує вдосконалення. Чинні Методичні рекомендації³³⁶ не враховують таких факторів, як вигоди і переваги відкритого використання відомостей, що підлягають віднесенню до державної таємниці; витрати на захист

таких відомостей порівняно зі збитками, що можуть бути завдані у разі їх розголошення.

Окремому розгляду підлягають проблеми, пов'язані з віднесенням відомостей до інших передбачених законодавством таємниць, конфіденційної інформації та критерії визначення їх конфіденційності.

Чинним законодавством визначено близько двох десятків таємниць та декілька видів конфіденційної інформації. Такий перелік видів інформації з обмеженим доступом викликає ряд запитань. Які грифи обмежень доступу або обмежувальні позначки треба надавати матеріальним носіям кожного виду інформації з обмеженим доступом? Законом України «Про державну таємницю» заборонено надавати грифи секретності, передбачені цим законом, матеріальним носіям іншої таємної інформації, яка не становить державної таємниці, або конфіденційної інформації. Як здійснювати узгодження ступенів обмеження доступу до різних видів інформації з обмеженим доступом у процесі обміну ними між суб'єктами інформаційної діяльності України та в процесі міжнародного інформаційного співробітництва? Відповідно до стандартів Європейського Союзу легітимними визнаються лише ступені обмеження доступу до інформації, встановлені національними законами.

Ступінь обмеження доступу і гриф, який відповідає цьому ступеню обмеження, завжди визначають важливість інформації та рівень її охорони з боку держави і власника. А це веде до питання про можливість в організаційному, правовому, методичному й економічному планах сформувати загальну систему охорони інформації.

Нагадаємо, що ступінь секретності та конфіденційності і відповідні їм грифи обмеження доступу є важливими елементами правового режиму інформації і встановлюються нормами законів. Обмеження доступу до будь-якої інформації, визначені підзаконними актами, є нелегітимними.

Незважаючи на це, у листопаді 1998 року постановою Кабінету Міністрів України «Про затвердження Інструкції про порядок зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, яка є власністю держави», запропоновано міністерствам, іншим центральним органам виконавчої влади,

Раді міністрів Автономної Республіки Крим, обласним, Київській та Севастопольській міським державним адміністраціям у межах їхніх повноважень розробити і ввести в дію переліки конфіденційної інформації, що є власністю держави. Також встановлено, що у разі потреби на державних підприємствах, в установах і організаціях з урахуванням їхньої діяльності розробляються та за погодженням з міністерством, іншим центральним органом виконавчої влади, до сфери управління якого вони належать, вводяться в дію відповідні переліки інформації³³⁷. Як відомо, запропоновані переліки конфіденційної інформації, що є власністю держави, розроблено і введено в дію; тобто обмеження на доступ до вказаної інформації введено на рівні вимог підзаконного акта, що суперечить правовій нормі Конституції України (ст. 34) про те, що обмеження прав на інформацію може бути встановлено тільки законом.

Наведені переліки відомостей, підстави і критерії віднесення їх до інформації з обмеженим доступом можуть визначатися лише на підставі вимог відповідних законів, якими встановлюється правовий режим кожного виду такої інформації.

Ця проблема може бути розв'язана прийняттям ряду законів про конкретні види таємниць або окремого Закону «Про інформацію з обмеженим доступом», що стануть правовою базою для розробки і впровадження підстав, процедур і методик віднесення відомостей до конкретних таємниць і конфіденційної інформації та впровадження режиму конфіденційності.

На сьогодні віднесення відомостей до інформації з обмеженим доступом, що не становить державної таємниці, здійснюється на підставі відомчих методик, різних за змістом щодо їх вимог, критеріїв і процедур. А в окремих випадках ці питання вирішуються відповідно до методик радянських часів. Європейський вибір України, реалізація Концептуальних засад стратегії економічного та соціального розвитку України на 2002 — 2011 роки, визначених у травневому посланні Президента України до Верховної Ради України, потребують невідкладної гармонізації національного законодавства з правовими нормами, прийнятими в державах ЄС щодо гарантування інформаційних прав і свобод та порядку їх обмежень в інтересах національної безпеки та іншої суспільної необхідності.

Загалом в Україні створена й функціонує структурно визначена система забезпечення інформаційної безпеки та безпеки сфери обігу інформації. Функції та повноваження відповідних державних органів закріплено в нормативно-правових актах різного рівня — Конституції України, законах України, указах Президента України, постановах Кабінету Міністрів України, інших, у тому числі відомчих, нормативних актах. Водночас розподіл функцій між окремими суб'єктами права в системі та схема їх взаємодії потребують удосконалення та врахування важливих як внутрішніх, так і зовнішніх чинників.

Проблемні аспекти ключових напрямів державної політики щодо інформаційної безпеки всебічно обґрунтовані у монографії Національного інституту стратегічних досліджень «Стратегії розвитку України: теорія і практика» (за ред. О. С. Власюка). Автори розділу монографії (О. Г. Додонов, О. В. Литвиненко, С. О. Янішевський) ґрунтовно доводять³³⁸, що, попри певні зрушення у розвитку національного інформаційного простору та нормативно-правове забезпечення інформаційних відносин, загальна ситуація в інформаційній сфері не відповідає сучасним вимогам, інтересам суспільства і держави. Серед негативних чинників автори визначають такі:

- найнебезпечнішим явищем є тенденція до прогресуючого відставання України від провідних країн світу в рівні та темпах розвитку національних інформаційних ресурсів та відповідної інфраструктури;

- неадаптованість інформаційної сфери країни до процесів глобалізації та невиваженість державної інформаційної політики створює загрозу обмеження суверенітету країни;

- недостатня увага до проблем захисту інформаційної інфраструктури та інформаційних ресурсів ускладнює діяльність держави щодо забезпечення національної безпеки і обороноздатності держави³³⁹.

- За сучасних умов посилення інформаційного протиборства потребує подальшого удосконалення система захисту інформації у спеціальних телекомунікаційних системах зв'язку та системах зв'язку загального користування.

Відсутність цілісної системи інформаційно-аналітичного забезпечення органів державної влади також значно ускладнює

прийняття ними виважених рішень, породжує конфліктні ситуації у владних структурах і в суспільстві.

Недостатнє інформаційно-аналітичне забезпечення своєї діяльності є характерним для всіх державних органів — як на центральному рівні, так і в регіонах. Владні структури не мають достатніх можливостей завчасно прогнозувати розвиток подій в Україні та навколо неї, належним чином враховувати сприятливі та обмежувальні чинники, що визначають результативність прийнятих політичних рішень, здійснювати планування навіть на середньострокову перспективу.

Створення інформаційно-аналітичних підрозділів дотепер не має системного характеру, а в ході чергового скорочення чисельності державних органів окремі з них взагалі ліквідуються. Наявні інформаційно-аналітичні підрозділи, які підтримують роботу різних органів державної влади, організаційно й функціонально роз'єднані, не забезпечують належної інформаційної взаємодії органів влади. Інформаційні мережі створюються на різних засадах щодо програмного, технічного, лінгвістичного забезпечення. На сьогодні вже створено ряд мереж передавання даних Міністерства палива і енергетики, Міністерства транспорту, Міністерства освіти і науки, Державного митного комітету та інших відомств, однак вони не мають горизонтальних зв'язків, що значно обмежує їхню ефективність.

Остаточно не узгоджено програмно-технічні аспекти створення систем інформаційно-аналітичного забезпечення органів державної влади. Державні структури здійснюють закупівлю комп'ютерів, програмного забезпечення різних типів, часто несумісних один з одним. Це ускладнює (іноді унеможлиблює) повноцінний обмін інформацією між відомствами, ставить під сумнів можливість створення цілісної інформаційно-аналітичної системи.

Відсутня єдина національна система класифікації інформації, суттєвого вдосконалення потребує система стандартизації та сертифікації. Наприклад, з 2000 стандартів у галузі інформаційних технологій Міжнародної організації зі стандартизації (ISO) Україною впроваджено близько 100 стандартів, причому переважно тих, що стосуються термінології. У країні дотепер діють колишні радянські стандарти (системи ГОСТ), неузгоджені з міжнародно-правовими актами.

Необхідне вдосконалення національної системи статистичної звітності. Впровадження системи узгоджених показників, за якими має опрацьовуватися змістовна інформація, є завданням виключної важливості: використання неповної та/або недостовірної інформації спричиняє ухвалення помилкових рішень, що обертаються втратами для суспільства і держави.

Концепція (Основи державної політики) національної безпеки України, схвалена Верховною Радою України 1997 року, є основою для формування відповідної законодавчої бази, підготовки доктрин, стратегій, концепцій, державних і відомчих програм у різних сферах національної безпеки, в тому числі в інформаційній сфері. Як підтвердила практика, такі положення залишаються виключно деклараціями, якщо не визначено механізми втілення їх у життя.

Таким чином, підсумовуючи, доцільно підкреслити, що в сучасних умовах проблеми забезпечення інформаційної безпеки та сфери обігу інформації набувають надзвичайно гострого звучання та нового забарвлення і потребують підвищення дієздатності в цій сфері держави та уваги до розв'язання зазначених проблем державних органів.

3.2. СТРАТЕГІЯ УПРАВЛІННЯ НАЦІОНАЛЬНИМИ ІНФОРМАЦІЙНИМИ РЕСУРСАМИ: МОДЕЛЬ СИСТЕМНОЇ ТРАНСФОРМАЦІЇ

Удосконалення системи державного управління національними інформаційними ресурсами безпосередньо залежатиме від визначення її цілей, як це достатньою мірою обґрунтовано в закордонних і вітчизняних наукових працях. Визначення мети завжди потребує перетворення її у дію, тобто визначення функцій структурних елементів системи.

У першому розділі даної монографії ми розглянули національні моделі становлення інформаційного суспільства в різних країнах світу і звернули увагу на те, що політична стратегія ЄС на цьому напрямі забезпечує провідну роль держави у перехідний період, яка виступає гарантом інтересів суспільства в умовах становлення інформаційної економіки та розширення сфери інформаційних послуг на всіх рівнях життєдіяльності держави³⁴⁰.

У сучасних умовах стає дедалі очевиднішим, що інформаційні ресурси є одним з визначальних факторів розвитку суспільства й країни, а широкий доступ і ефективне використання накопичених інформаційних ресурсів у науково-технологічній, виробничій, управлінській та інших видах повсякденної ділової діяльності особи, суспільства і держави є важливим показником статусу країни у світовому співтоваристві.

Національні інформаційні ресурси України складаються з мільйонів окремих документів і масивів документів як традиційних — у паперовому вигляді, так і на електронних носіях, баз і банків даних, бібліотечних, архівних, музейних, картографічних фондів, реєстрів, кадастрів та інших, що містять дані, відомості, знання, пов'язані з усіма сферами життя людини, суспільства й держави. За нашими оцінками, більше третини національних інформаційних ресурсів, створених на кошти державного бюджету, позабюджетних державних фондів та платників податків, є власністю держави. Потенціал інформаційних ресурсів України поки що займає одне з провідних місць не тільки у країнах СНД, а й у світі, однак показники, що характеризують доступність користувачів до інформаційних ресурсів України та ефективність їхнього використання, з різних причин значно відстають від розвинутих країн. Однією з таких причин є недосконалість системи державного управління національними інформаційними ресурсами³⁴¹.

Головну мету державної інформаційної політики стосовно національних інформаційних ресурсів можна сформулювати як створення необхідних економічних і соціокультурних умов та правових і організаційних механізмів формування, розвитку і забезпечення ефективного використання національних інформаційних ресурсів у всіх сферах життя і діяльності громадянина, суспільства і держави.

Відповідно до головної мети державної інформаційної політики щодо національних інформаційних ресурсів можна сформулювати функції державного управління цією сферою діяльності, а саме:

— розробка й прийняття політичних рішень, законодавчих і нормативно-правових актів щодо правового забезпечення системи управління національними інформаційними ресурсами та

удосконалення правових і організаційних механізмів реалізації правових норм чинного законодавства;

— визначення і здійснення повноважень державних органів, органів регіонального й місцевого самоврядування щодо оперативного управління (володіння, розпорядження, користування) державними інформаційними ресурсами;

— розробка і реалізація організаційних і нормативно-методичних заходів для координації діяльності відомчих і регіональних структур та недержавного сектору в сфері формування й використання інформаційних ресурсів;

— розробка і реалізація фінансово-економічних методів регулювання діяльності щодо формування й забезпечення використання інформаційних ресурсів;

— забезпечення державної реєстрації інформаційних ресурсів, повноти створення первинних і похідних інформаційних ресурсів на основі інформації, що розробляється (створюється) у процесі діяльності державних органів, органів регіонального і місцевого самоврядування, підприємств, установ і організацій незалежно від форм власності;

— формування інформаційних ресурсів про діяльність державних органів, органів регіонального і місцевого самоврядування, державних підприємств і організацій з метою надання їх для вільного доступу громадянам і організаціям (крім тих інформаційних ресурсів, що мають відомості, віднесені до державної таємниці, та до іншої інформації з обмеженим доступом);

— забезпечення ефективного використання інформаційних ресурсів у діяльності державних органів, органів регіонального і місцевого самоврядування та державних підприємств, установ і організацій;

— оптимізація державної політики інформатизації щодо забезпечення науково-технічних, виробничо-технологічних і організаційно-економічних умов створення й застосування інформаційних технологій та інших елементів інформаційної інфраструктури ДІА формування, розвитку й ефективного використання інформаційних ресурсів та сприяння доступу громадян до світових інформаційних ресурсів, глобальних інформаційних систем;

— забезпечення функціонування ефективно діючої системи захисту інформаційних ресурсів;

— забезпечення захисту громадян, суспільства й держави від хибної, спотвореної та недостовірної інформації;

— забезпечення розробки і впровадження ефективних правових, організаційних і економічних механізмів регулювання інформаційних ресурсів України (ринку інформації, інформаційних технологій, засобів обробки інформації та інформаційних послуг);

— регулювання інформаційного співробітництва, спрямованого на забезпечення рівноправного і взаємовигідного використання національних інформаційних ресурсів у процесі міжнародного обміну;

— здійснення єдиної державної політики наукового забезпечення системи державного управління формуванням, розвитком і використанням національних інформаційних ресурсів;

— кадрове забезпечення функціонування системи державного управління національними інформаційними ресурсами;

— інформаційно-аналітичне забезпечення прийняття управлінських рішень у сфері управління інформаційними ресурсами;

— контроль за встановленим порядком і правилами формування, розвитку, поширення і використання інформаційних ресурсів;

— нагляд за додержанням законодавства в сфері формування, розвитку, поширення і використання інформаційних ресурсів та здійснення правосуддя у сфері суспільних інформаційних відносин.

Організаційно-правову систему державного управління і захисту інформаційних ресурсів можна подати у вигляді таблиць {табл. 3 — 6}.

Розглянемо функціональне навантаження структурних елементів організаційно-правової системи державного управління інформаційними ресурсами.

Верховна Рада України. Відповідно до Конституції України³⁴² «єдиним органом законодавчої влади в Україні є парламент — Верховна Рада України» (ст. 75). Тільки Верховна Рада України здійснює законодавче регулювання суспільних відносин, у тому числі в інформаційній сфері; визначає засади зовнішньої і внутрішньої політики; затверджує Державний бюджет України, в якому передбачає, зокрема, і кошти на розвиток інформаційної

Таблиця 3

Перший рівень системи державного управління інформаційними ресурсами

Суб'єкти першого рівня	Структури першого рівня управління	Функції структур першого рівня управління
1	2	3
Верховна Рада України: Здійснює законодавче регулювання суспільних інформаційних відносин	Профільні Комітети ВР України: з питань свободи слова та інформації; з питань оборони і національної безпеки	Здійснюють законопроектну роботу і попередньо розглядають питання, віднесені до повноважень Верховної Ради України згідно з компетенцією кожного профільного комітету
	Інститут законодавства ВР України	Здійснює наукове забезпечення законодавчої діяльності парламенту
	Інформаційно-аналітичне управління Апарату ВР України	Здійснює інформаційне забезпечення поточної роботи керівників парламенту, профільних Комітетів та народних депутатів України
	Консультативна Рада з питань інформатизації при ВР України	Розглядає проекти правових актів з питань інформатизації та проекти Національної програми інформатизації
Президент України	Адміністрація Президента України	Розробляє пропозиції, спрямовані на забезпечення виконання Президентом України повноважень, визначених Конституцією України, в тому числі щодо прийняття політичних рішень та нормативно-правового регулювання суспільних інформаційних відносин, пов'язаних із формуванням і використанням інформаційних ресурсів України та забезпеченням національної безпеки
	національний інститут стратегічних досліджень	Здійснює наукове аналітично- прогнозне супроводження діяльності Президента України

			Таблиця 4	
1	2	3	Другий рівень системи державного управління інформаційними ресурсами	
	Рада національної безпеки і оборони України	Координує і контролює діяльність органів виконавчої влади у сфері національної безпеки й оборони	Суб'єкти управління другого рівня (міністерства, відомства, інші центральні органи державної виконавчої влади)	
	Апарат РНБО України	Здійснює поточне організаційне та інформаційно-аналітичне забезпечення діяльності РНБО України	Виконання функцій структурними елементами другого рівня управління у сфері	
	Національний інститут проблем міжнародної безпеки	Забезпечує проведення фундаментальних та прикладних розробок з актуальних питань глобальної та регіональної безпеки		
	Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки при РНБО України	Здійснює аналіз стану і розроблення пропозицій щодо координації діяльності центральних державних органів з питань інформаційної політики та інформаційної безпеки		
	Секретаріат Управління інформаційних технологій	Здійснює заходи щодо впровадження інформаційних технологій у діяльність структурних підрозділів апарату Кабінету Міністрів України		
" " Кабінет Міністрів країни. Забезпечує державний суверенітет, здійснення внутрішньої та зовнішньої політики держави, виконання ... онституції і законів України, актів Президента країни	Урядова комісія з питань інформаційно-аналітичного забезпечення органів виконавчої влади	Розглядає проекти законодавчих, нормативно-правових актів з питань щодо інформаційної сфери та розробляє пропозиції щодо вдосконалення інформаційно-аналітичного забезпечення діяльності органів державної виконавчої влади		
			Не визначений	Здійснення загальнодержавних заходів організаційного, нормативно-методичного забезпечення, координації і контролю
			Не визначений	Державної реєстрації ІР загального доступу (формування державної бази метаданих)
			Не визначений	Державної реєстрації ІР, що містять державну таємницю та іншу інформацію з обмеженим доступом (база метаданих)
			Не визначений	Державної реєстрації інформаційних ресурсів, отриманих у процесі міждержавного інформаційного співробітництва (база метаданих)
			Не визначений	Обліку державних ІР як майна, порядку їх закріплення в оперативне управління і господарське відання
			Не визначений	Фінансування структур і процесів формування державних ІР, визначення порядку надання платних послуг, формування інформаційного ринку
			Держкомзв'язку та інформатизації України	Зв'язку та інформатизації
			Не визначений	Розробки інформаційних технологій та координації цієї діяльності
			Міністерство фінансів України	Фінансування матеріального виробництва, наукової та інших видів діяльності
			Національний банк України	Банківської справи
			Міністерство оборони України	Оборони
			Служба безпеки України	Державної безпеки
			Міністерство внутрішніх справ України	Боротьби зі злочинністю та охорони правопорядку
			Президія Національної академії наук України	Фундаментальних і пошукових наукових досліджень, координації наукової діяльності

1	2
Міністерство економіки та з питань європейської інтеграції України Міністерство промислової політики України	Матеріального промислового виробництва
Міністерство аграрної політики України	Аграрній
Держкомстат України	Державної статистики
Міністерство юстиції України	Правової інформації та реєстрації нормативно-правових документів
Міністерство закордонних справ України	Реєстрації міждержавних угод, координації міжнародного співробітництва
Національна Рада України з питань телебачення і радіомовлення Держкомітет телебачення і радіомовлення України	Друкованих засобів масової інформації, телебачення й радіомовлення, видавничої справи
Фонд держмайна України	Нерухомості та держмайна
Державна комісія з цінних паперів та фондового ринку України	Цінних паперів та фондового ринку
Укргеодезкартографія	Картографічної та геодезичної інформації
Міністерство праці України	Трудових ресурсів та охорони праці
Мінкультури і мистецтв України	Культури, бібліотечної та музейної справи
МОЗ України	Охорони здоров'я
Державне архівне відомство	Архівної справи
Держкомзем України	Земельних кадастрів та державної земельної політики

Ч

Таблиця 5
Визначені законодавчими та нормативно-правовими актами спеціально уповноважені державні органи

Спеціальні функції	Спеціально уповноважені державні органи — структурні елементи другого рівня управління — законодавчо визначені	Спеціально уповноважені державні органи — структурні елементи другого рівня управління — законодавчо не визначені
1	2	3
У сфері забезпечення охорони державної таємниці	Служба безпеки України	
У мережах передавання даних, технічного та криптографічного захисту інформації	Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України	
У сфері захисту інформаційного простору України, контролю за додержанням законодавства про державну таємницю у ЗМІ	Держкомітет телебачення і радіомовлення України	
У сфері охорони інформації з обмеженим доступом, що не становить державної таємниці		Не визначений
Нагляду за додержанням законодавства в інформаційній сфері	Органи прокуратури	
У сфері відповідності законодавчих та інших правових актів інформаційної сфери Конституції України	Конституційний Суд України	
Здійснення правосуддя у сфері суспільних інформаційних відносин	Суди загальної юрисдикції	
У сфері охорони носіїв інформації з обмеженим доступом під час їх транспортування	Держфельдслужба	
У сфері захисту особи, суспільства, держави від хибної, недостовірної, недоброякісної інформації		Не визначений

Таблиця 6

Третій рівень системи державного управління
інформаційними ресурсами

Структурні елементи	Функції, закріплені у нормативно-правовому порядку	
	визначені	не визначені
1	2	3
Органи державної влади, Міністерства, ІНШІ центральні органи виконавчої влади, органи місцевого і регіонального самоврядування	Створюють підрозділи, служби: інформаційно-аналітичного забезпечення; режиму, секретного діловодства, технічного захисту інформації та загального діловодства; прес-служби	Служби, системи, бази і банки даних для задоволення потреб громадян, юридичних осіб, держави
	Формування, поширення, використання та захист інформаційних ресурсів, які створено апаратами в процесі професійної діяльності, забезпечення державної реєстрації ІР	
Щодо об'єктів ІІІ рівня (підпорядкованих підприємств, установ, організацій) забезпечують:		
Органи державної виконавчої влади, міністерства, інші центральні органи виконавчої влади	Організаційне та методичне керівництво та відомчий контроль за виконанням встановленого порядку і правил формування, поширення, використання і захисту ІР, що належать до відповідної сфери управління	
Органи регіонального і місцевого самоврядування	Затверджують регіональні й місцеві програми розвитку інформаційної сфери, бюджети відповідних адміністративно-територіальних одиниць з урахуванням розвитку інформаційної сфери	

1	2	3
Рада міністрів Автономної Республіки Крим, обласні, Київська та Севастопольська міські державні адміністрації	Забезпечують виконання законодавчих та нормативно-правових актів на відповідних територіях, державних і регіональних програм розвитку інформаційної сфери Здійснюють територіальний контроль за виконанням порядку і правил формування, поширення, використання і захисту ІР	Формують регіональні місцеві реєстри ІР та забезпечують їх державну реєстрацію
Підприємства, установи, організації всіх форм власності	Формують інформаційні ресурси, створені в процесі професійної діяльності, відповідно до встановленого порядку і правил Забезпечують захист ІР з урахуванням специфіки діяльності та створюють відповідні служби режиму, діловодства, технічного захисту інформації	Подають інформаційні ресурси, створені в процесі професійної діяльності, відповідно до встановленого порядку і правил на державну реєстрацію

сфери; затверджує загальнодержавні програми економічного, науково-технічного, соціального, національно-культурного розвитку; надає згоду на обов'язковість міжнародних договорів України, в тому числі щодо міжнародного інформаційного співробітництва; здійснює парламентський контроль у межах, визначених Конституцією України (ст. 85).

Конституційними правовими нормами встановлено, що «виключно законами України визначаються права і свободи людини й громадянина, гарантії цих прав і свобод» (ст. 92). Виключно законами України визначається також правовий режим власності, організація державної статистики та інформатики, основи національної безпеки (ст. 92).

Профільні Комітети Верховної Ради України здійснюють законопроектну роботу і попередньо розглядають питання, віднесені до повноважень Верховної Ради України згідно з компетенцією кожного профільного комітету.

Консультаційна рада з питань інформатизації при Верховній Раді України розглядає проекти правових актів з питань інформатизації та проекти Національної програми інформатизації.

Інститут законодавства Верховної Ради України здійснює наукове забезпечення законодавчої діяльності парламенту.

Інформаційно-аналітичне управління Апарату Верховної Ради України здійснює інформаційне забезпечення поточної роботи керівників парламенту, профільних Комітетів та народних депутатів України.

Президент України відповідно до Конституції України як глава держави є гарантом державного суверенітету, територіальної цілісності України, додержання Конституції України, прав і свобод людини й громадянина (ст. 102). Згідно з конституційними повноваженнями Президент забезпечує національну безпеку і здійснює керівництво у цій сфері діяльності, в тому числі в сфері забезпечення інформаційного суверенітету та національної безпеки як важливих складових національної безпеки; звертається з посланнями до народу та із щорічними посланнями до Верховної Ради України про внутрішнє й зовнішнє становище України, в тому числі в інформаційній сфері; здійснює керівництво зовнішньополітичною діяльністю держави; створює, реорганізовує та ліквідує міністерства та інші центральні органи виконавчої влади; призначає за поданням Прем'єр-міністра та звільняє з посад керівників міністерств, державних комітетів, інших центральних органів, в тому числі органів виконавчої влади, що здійснюють повноваження в інформаційній сфері (ст. 106).

Адміністрація Президента України розробляє пропозиції, спрямовані на забезпечення виконання Президентом України повноважень, визначених Конституцією України, зокрема, щодо прийняття політичних рішень та нормативно-правового регулювання суспільних інформаційних відносин, пов'язаних із формуванням і використанням інформаційних ресурсів України та забезпеченням національної безпеки.

Національний інститут стратегічних досліджень при Президенті України здійснює наукове аналітично-прогнозне супроводження діяльності Президента України.

Рада національної безпеки і оборони (РНБО) України відповідно до Конституції України є координаційним органом з питань національної безпеки й оборони України при Президенті України. РНБО України координує і контролює діяльність органів виконавчої влади у сфері національної безпеки й оборони (ст. 107).

Законом України «Про Раду національної безпеки і оборони України», прийнятим у березні 1998 року, на РНБО України покладено виконання таких функцій: внесення пропозицій Президенту України щодо реалізації засад внутрішньої і зовнішньої політики в сфері національної безпеки і оборони; координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки й оборони в мирний час; координація та здійснення контролю за діяльністю органів виконавчої влади в сфері національної безпеки і оборони в умовах воєнного або надзвичайного стану та під час виникнення кризових ситуацій, що загрожують національній безпеці України.

Відповідно до функцій, визначених законом України, РНБО України подає главі держави пропозиції щодо стратегічних національних інтересів України та концептуальних підходів та напрямів забезпечення національних інтересів України у всіх сферах життя і діяльності суспільства і держави, в тому числі забезпечення інформаційної безпеки; утворення, реорганізації та ліквідації органів державної виконавчої влади; проекту державного бюджету за статтями, пов'язаними із забезпеченням національної безпеки і оборони України; заходів політичного, соціального, воєнного, науково-технологічного, екологічного, інформаційного та іншого характеру відповідно до масштабу потенційних та реальних загроз національним інтересам України.

Апарат Ради національної безпеки і оборони України здійснює поточне організаційне та інформаційно-аналітичне забезпечення діяльності РНБО України.

Національний інститут проблем міжнародної безпеки забезпечує проведення фундаментальних та прикладних розробок з актуальних питань глобальної та регіональної безпеки, участі України в системі багатосторонніх та двосторонніх міждержавних відносин.

Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки при РНБО України здійснює аналіз стану і розробляє пропозиції щодо координації діяльності центральних державних органів з питань інформаційної політики та інформаційної безпеки.

Кабінет Міністрів України відповідно до конституційних правових норм забезпечує державний суверенітет, здійснення внутрішньої та зовнішньої політики держави, виконання Конституції і законів України, актів Президента України; вживає заходів щодо забезпечення прав і свобод людини і громадянина; забезпечує проведення фінансової, цінової, інвестиційної та податкової політики; розробляє і здійснює загальнодержавні програми економічного, науково-технічного, соціального і культурного розвитку України; забезпечує рівні умови розвитку всіх форм власності; здійснює управління об'єктами державної власності³⁴³, розробляє Державний бюджет України і забезпечує виконання затвердженого Верховною Радою України Державного бюджету України; здійснює заходи для забезпечення обороноздатності і національної безпеки України; організовує і забезпечує здійснення зовнішньоекономічної діяльності України; спрямовує і координує роботу міністерств, інших органів виконавчої влади (ст. 116).

Урядова комісія з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади розглядає проекти законодавчих, нормативно-правових актів інформаційної сфери та розробляє пропозиції щодо вдосконалення інформаційно-аналітичного забезпечення діяльності органів державної виконавчої влади.

Управління інформаційних технологій Секретаріату Кабінету Міністрів України здійснює заходи, спрямовані на впровадження інформаційних технологій у діяльність структурних підрозділів апарату Кабінету Міністрів України.

Як зазначалося, рівень прийняття політичних рішень, законодавчого і нормативно-правового забезпечення державної інформаційної політики управління національними інформаційними ресурсами України є стратегічним. На цьому рівні визначаються національні інтереси та їхні пріоритети в інформаційній сфері; формуються правові засади для побудови, розвитку системи національних інформаційних ресурсів та управлін-

ня цією системою; на основі головної стратегічної мети державної інформаційної політики щодо інформаційних ресурсів визначаються функції та їх раціональне розподілення між організаційними структурами, що створюються для досягнення стратегічних цілей; формуються основні правові й організаційні засади кадрового, фінансового, матеріально-технічного, інформаційного та інших видів стратегічного забезпечення системи управління національними інформаційними ресурсами; здійснюється стратегічне прогнозування розвитку інформаційної сфери та прийняття політичних і політико-правових рішень для удосконалення системи управління цією сферою.

Функції стратегічного рівня, що належать Верховній Раді України, Президентові України, Раді національної безпеки і оборони України та Кабінетові Міністрів України, впливають із повноважень цих вищих державних органів, визначених конституційними правовими нормами.

Реальністю є те, що законопроекти, спрямовані на регулювання відносин в інформаційній сфері, розробляються за ініціативою комітетів Верховної Ради України, державних органів, а в деяких ситуаційно зумовлених випадках — за дорученням Президента України та Кабінету Міністрів України. У проекті Концепції реформування законодавства України у сфері суспільних інформаційних відносин з цього приводу зазначається: «Правотворчий процес нерідко здійснюється шляхом вирішення окремих проблем в окремих законах та підзаконних актах фрагментарно». І далі: «Правотворчий процес нерідко здійснюється без узгодження з чинним законодавством, не враховується специфіка національної ментальності, правової культури систематизації права, які є основою правосвідомості населення, інші особливості соціального і державного життя»³⁴³.

Окрім того, важливим аспектом цієї проблеми є те, що чинні акти законодавства інформаційної сфери, особливо проекти законодавчих актів, у тому числі проект Інформаційного кодексу України³⁴⁴, проект Закону України «Про національні інформаційні ресурси»³⁴⁵, щодо свободи інформаційної діяльності та права на інформацію, є декларативними у зв'язку з невизначеністю правових механізмів гарантування цих прав і свобод, а також із відсутністю кореляції їх з обов'язками і відповідальністю державних органів і юридичних осіб стосовно формування

інформаційних ресурсів, передбачених для задоволення інформаційних потреб суб'єктів України.

Недостатня послідовність і системність правотворчого процесу на законодавчому рівні створюють і надалі створюватимуть певні проблеми щодо регулювання суспільних інформаційних відносин та удосконалення системи управління інформаційними ресурсами на рівні політико-правових рішень, що приймаються Президентом України, та нормативно-правових актів, які затверджуються Кабінетом Міністрів України.

Означене є підставою для висновку про те, що на стратегічному рівні залишається актуальною координація правотворчого процесу стосовно формування правових засад побудови, забезпечення функціонування й розвитку системи управління інформаційними ресурсами України.

Відповідно до Конституції України основні важелі державного керівництва у сфері національної безпеки, зокрема інформаційної безпеки та інформаційного суверенітету, основу яких становлять національні інформаційні ресурси (формування, розвиток, захист, рівноправне і взаємовигідне використання в процесі міжнародного співробітництва), віднесено до повноважень Президента України.

Президент України вживає активних заходів для вдосконалення системи управління інформаційною сферою. Важливе політико-правове значення мають Укази Президента України «Про деякі заходи щодо захисту держави в інформаційній сфері» від 22 квітня 1998 року; «Про вдосконалення державного управління інформаційною сферою» від 16 вересня 1998 року; «Про вдосконалення інформаційно-аналітичного забезпечення Президента України та органів державної влади» від 14 липня 2000 року; «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі» від 31 липня 2000 року; «Про додаткові заходи щодо безперешкодної діяльності засобів масової інформації, дальшого утвердження свободи слова в Україні» від 9 грудня 2000 року; «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» від 23 серпня 2001 року та ін.

Пропозиції для прийняття Президентом України політичних і політико-правових рішень стосовно визначення стратегічних національних інтересів в інформаційній сфері, управління цією сферою, в тому числі формуванням, розвитком, поширенням і використанням національних інформаційних ресурсів та їх захистом розробляються Адміністрацією Президента України, а також схвалюються у рішеннях РНБО України. Відповідно до Конституції України (ст.106) Президент України утворює, реорганізовує та ліквідовує міністерства та інші органи виконавчої влади за поданням Прем'єр-міністра України. Пропозиції про організаційні зміни у системі органів виконавчої влади розробляються структурними підрозділами апарату Кабінету Міністрів України.

За оцінками експертів, органи виконавчої влади, що забезпечують реалізацію державної інформаційної політики у сфері, пов'язаній з управлінням і захистом інформаційних ресурсів, перебувають у стадії перманентної реорганізації. Складається таке враження, що пропозиції про черговий етап адміністративної реформи розробляються, виходячи не із функцій державного управління інформаційною сферою, а на основі арифметичних підходів: бюджетні кошти — чисельність працівників — матеріально-технічне забезпечення.

Наслідком таких підходів є те, що в процесі реформування державних органів була втрачена важлива функція державного управління, пов'язана із розробкою і впровадженням організаційних, нормативно-методичних заходів, координації і контролю захисту інформаційних ресурсів з обмеженим доступом, що не становлять державної таємниці. Виконання вказаних функцій у 1993 році було покладене на утворений у той час Державний комітет по охороні державних таємниць у пресі та інших засобах масової інформації³⁴⁶.

На правонаступника цього комітету (Держкомінформполітики, телебачення і радіомовлення України) Законом України «Про державну таємницю» покладена лише функція контролю за додержанням законодавства про державну таємницю з метою запобігання її поширенню у пресі та інших засобах масової інформації³⁴⁷.

На другому рівні державного управління, на якому центральними органами виконавчої влади здійснюється організацій-

не, нормативно-методичне забезпечення виконання законодавчих актів, політичних і політико-правових рішень Верховної Ради України, Президента України, Кабінету Міністрів України, а також координація і контроль за формуванням, поширенням, використанням та захистом інформаційних ресурсів, *важливі функції досі залишаються не визначеними, а саме:*

- здійснення загальнодержавних заходів організаційного, нормативно-методичного забезпечення, координації і контролю; планування конкретних заходів і оперативне управління системою та її структурними елементами;

- *— організація державної реєстрації відкритих інформаційних ресурсів, формування державного реєстру бази метаданих, до якого доцільне включення як даних державного реєстру, так і регіональних реєстрів баз метаданих;

- організація державної реєстрації інформаційних ресурсів, що містять державну таємницю та іншу інформацію з обмеженим доступом;

- організація державної реєстрації інформаційних ресурсів, отриманих у процесі міжнародного співробітництва (окремо — відкритих інформаційних ресурсів і окремо — інформаційних ресурсів з обмеженим доступом);

- ведення обліку державних інформаційних ресурсів як майна або немайнових активів, впровадження порядку їх закріплення в оперативне управління і господарське відання;

- фінансування заходів з формування державних інформаційних ресурсів, визначення порядку надання платних послуг на основі опрацювання державних інформаційних ресурсів та формування інформаційного ринку;

- організація розробки інформаційних технологій, їх державна реєстрація та державна координація цієї діяльності;

- розробка і впровадження організаційних, нормативно-методичних заходів, координація і контроль у сфері охорони інформації з обмеженим доступом, що не становить державної таємниці;

- організаційне, нормативно-методичне забезпечення, координація і контроль за реалізацією державної інформаційної політики в сфері захисту особи, суспільства й держави від хибної, недостовірної, недоброякісної інформації, тобто забезпе-

чення інформаційної безпеки у широкому розумінні цього поняття.

На другому і третьому рівнях державного управління і захисту інформаційних ресурсів курсивом позначені функції, які не визначені на державному рівні і не виконуються в державі; тобто, *починаючи з рівня виконавчої влади, не утворена ієрархічна вертикаль формування, поширення і використання інформаційних ресурсів та відсутні деякі елементи функціональної організаційно-правової системи управління і захисту інформаційних ресурсів.*

Важливою проблемою залишається ресурсне забезпечення державної інформаційної політики щодо формування, поширення, використання і захисту інформаційних ресурсів України.

Зазначимо, що повноваження вищих державних органів, визначені Конституцією України, зокрема, Верховної Ради України (ст.85), Президента України (ст.106), Ради національної безпеки і оборони України (ст.107), Кабінету Міністрів України (ст.116), дають змогу впровадити виважену державну інформаційну політику управління інформаційними ресурсами України.

Водночас загроза національній безпеці України в інформаційній сфері, визначена в Концепції (Основах державної політики) національної безпеки України, пов'язана з невиваженістю державної політики в цій сфері, залишається й досі. Схвалений Верховною Радою України у січні 1997 року, цей важливий документ не забезпечив поєднання підходів як до формування законодавчої бази, створення правових засад для побудови, функціонування і розвитку системи, так і до організаційного забезпечення, чіткого визначення функцій та раціонального їх розподілення між елементами системи та реалізації всього комплексу стратегічних завдань зміцнення національної безпеки України в інформаційній сфері. Державне управління сферою, основу якої становлять інформаційні ресурси України, залишається найбільш неврегульованою сферою державної управлінської діяльності.

Прийняті за останні роки закони, Укази Президента України та нормативно-правові акти Кабінету Міністрів України не забезпечують у правовому й організаційному відношенні формування і розвиток цілісної системи державного управління і захисту інформаційних ресурсів. Вони лише фрагментарно

передбачають розв'язання згаданих проблем і проектів актів законодавства, що розробляються або перебувають на розгляді у Верховній Раді України, в тому числі проекти Інформаційного кодексу України і Закону України «Про національні інформаційні ресурси».

Практика минулих років свідчить про те, що потребує суттєвого вдосконалення взаємодія, скоординованість і узгодженість дій і рішень парламенту — Президента — уряду з питань виконання конституційних повноважень щодо формування і реалізації державної інформаційної політики; на часі внесення докорінних змін до підходів проведення адміністративної реформи, спрямованих на забезпечення формування цілісної і стабільної структури органів виконавчої влади, виходячи із функцій і повноважень державних органів, закріплених у Конституції України, законах України, указах Президента України, постановах Кабінету Міністрів України, інших правових актах та удосконалення правових засад функціонування системи управління і захисту інформаційних ресурсів України.

3.3. ОРГАНІЗАЦІЙНІ ОСНОВИ ВДОСКОНАЛЕННЯ СИСТЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РЕСУРСАМИ

Відповідно до головної мети державної інформаційної політики щодо інформаційних ресурсів України обов'язком держави є створення системи організаційного забезпечення функціонування та удосконалення державного управління цією системою.

Організаційною основою системи управління інформаційними ресурсами доцільно вважати організовану сукупність центральних державних органів, органів регіонального і місцевого самоврядування, їхніх спеціальних підрозділів і служб та посадових осіб, юридичних осіб (підприємств і установ та інших господарюючих об'єктів), громадських організацій та окремих громадян, об'єднаних цілями та завданнями щодо формування, зберігання, поширення і забезпечення використання інформаційних ресурсів для задоволення інформаційних потреб особистості, суспільства й держави в межах чинного законодавства України.

Сьогодні можна вести мову лише про логічність побудови і можливість удосконалення організаційної системи управління і захисту інформаційних ресурсів, що містять державну таємницю. Спеціальним актом законодавства визначені повноваження державних органів, починаючи від формування державної політики у цій сфері — до компетенції посадових осіб та спеціальних підрозділів суб'єктів України, діяльність яких пов'язана з державною таємницею. На рівні закону визначена компетенція уряду щодо встановлення єдиних вимог до виготовлення, обліку, користування, зберігання, охоронності, передавання та транспортування матеріальних носіїв секретної інформації³⁴⁸.

Низкою нормативних документів, затверджених Президентом України, Кабінетом Міністрів України визначена компетенція ієрархічної структури суб'єктів щодо охорони державної таємниці на таких важливих напрямках діяльності, як міжнародне співробітництво та обробка секретної інформації в автоматизованих системах. Водночас аналіз організаційної структури управління інформаційною сферою, в тому числі інформаційними ресурсами України, функцій, які виконують державні органи та інші суб'єкти інформаційної діяльності щодо формування, поширення, використання та захисту інформаційних ресурсів, є підставою для таких висновків.

Перший. В Україні створено певну структуру державних органів для впровадження державної інформаційної політики управління інформаційними ресурсами та забезпечення інформаційної безпеки у цій сфері, тобто безпеки як інформаційних ресурсів, так і сфери їх обігу.

Водночас у державі залишається Реформованою загальнодержавна система управління і захисту інформаційних ресурсів, не об'єднані єдиною метою та завданнями державної інформаційної політики державні органи, що входять до цієї структури: Державний комітет телебачення і радіомовлення України, Державний комітет зв'язку та інформатизації України, Національна рада України з питань телебачення і радіомовлення, Міністерство освіти і науки України, Міністерство культури і мистецтв України, Служба безпеки України, а також міністерства і відомства, що здійснюють міжгалузеве та відомче управління певними видами інформаційних ресурсів: Міністерство економіки та з питань європейської інтеграції України, Міністерство юс-

тиції України, Державний комітет статистики України, Міністерство промислової політики України, Міністерство аграрної політики України та ін.

Реальністю є те, що в державі створена та діє громіздка та розпорошена структура державних органів управління і захисту інформаційних ресурсів. Ця структура дає змогу здійснювати формування інформаційних ресурсів за окремими напрямками за міжвідомчими ознаками, а щодо більшості видів інформаційних ресурсів діють відомчі підходи та інтереси. За межами впливу держави залишається організація розробки та впровадження єдиних загальнодержавних методичних та методологічних підходів, правил та порядку управління інформаційними ресурсами. Без визначення на рівні державної виконавчої влади державного органу з функціями організаційного, науково-методичного забезпечення виконання законодавчих і нормативно-правових актів, координації і контролю за формуванням, поширенням, використанням та захистом інформаційних ресурсів є проблематичним створення логічно завершеної системи управління цією сферою.

Другий. У нашій країні склалася хибна практика формування організаційної структури державних органів, що здійснюють управління конкретними напрямками інформаційної діяльності, — сфери найбільш чутливої і вразливої як для негативних внутрішніх, так і зовнішніх впливів. Спочатку формується організаційна структура органів державної виконавчої влади, а потім робиться спроба раціонально розподілити функції між ними. Фактично ігнорується дія об'єктивної закономірності, відповідно до якої стабільна організація управління системою та окремими напрямками її діяльності може бути досягнута тільки в тому разі, якщо організаційна структура формується, виходячи з функцій державного управління, а не навпаки. Так, Положення про Державний комітет зв'язку та інформатизації України було затверджене через півроку (3 червня 2000 року) після рішень про черговий етап адміністративної реформи, а про Державний комітет інформаційної політики, телебачення і радіомовлення України — ще пізніше (25 липня 2000 року). У деяких випадках визначення й закріплення у відповідних нормативних документах функцій державних органів залежить не від загальнодержавних цілей та інтересів, а від авторитету і

440

спроможностей знову призначених їхніх керівників обґрунтувати функції підпорядкованої їм структури у вищих державних органах, з якими узгоджуються вказані документи. Такий порядок є однією з головних причин того, що в процесі реформування державних органів створюються умови для втрати деяких функцій управління інформаційною сферою.

Суттєвим чинником негативного впливу на стан формування, поширення, використання і захисту інформаційних ресурсів є вкрай недосконала ієрархічна структура управління згаданими процесами. Міністерства і відомства як у центральних апаратах, так і на підприємствах, в установах і організаціях, що належать до сфери їх управління, створюють спеціальні підрозділи і служби, виходячи з залишкового принципу їх фінансування. У процесі чергових реорганізацій такі підрозділи та служби скорочуються або ліквідовуються в першочерговому порядку. Правовий статус і матеріальне забезпечення працівників таких підрозділів і служб на кілька порядків нижчі від інших підрозділів, а це породжує проблему комплектування їх кваліфікованими спеціалістами.

Організаційні і правові заходи, що вживаються державними органами для удосконалення системи управління і захисту інформаційних ресурсів, дають змогу лише «косметично» підправити деякі фрагменти цієї системи.

Третій. Підходи, на основі яких формується організаційна структура державних органів та визначаються їхні функції, були притаманні державній інформаційній політиці колишнього СРСР, основу якої складали агітація і пропаганда, діяльність засобів масової інформації. Інформаційні ресурси щодо результатів наукових досліджень і розробок, матеріального виробництва, а також інших сфер використовувалися лише в агітаційно-пропагандистських цілях для обґрунтування переваг соціалізму, викривання недоліків і критики капіталізму. Інформаційні ресурси деяких напрямів досліджень засекречувалися до 95% від їх загальних обсягів, поширення і використання цих ресурсів регламентувалося закритими підзаконними нормативними актами. Ця сфера була закрыта не тільки для широкого загального доступу — був обмежений обмін інформаційними ресурсами між міністерствами й відомствами. Зниження загальних темпів розвитку економіки колишнього СРСР зумовлено, серед інших

причин, і такою політикою щодо інформаційних ресурсів. Важливо зазначити, що на той час на інформаційні ресурси існувала єдина форма власності — державна, яка дуже чутлива до рішень держави як суб'єкта управління.

У сучасних умовах в Україні фактично сформовано ринкову економіку. Органи виконавчої влади для управління всіма сферами державного будівництва в нових умовах господарювання, в тому числі й ті, що здійснюють приватизацію й роздержавлення власності, координують підприємництво і підприємницьку діяльність, впроваджують антимонопольні заходи та ін. У країні поряд з державною власністю формується індивідуальна (особиста й приватна трудова) та приватна колективна. Здійснюється широка комерціалізація усіх сфер економічної діяльності.

Процес переходу від тоталітарного режиму і загальної системи засекреченості до ринкових перетворень не був забезпечений створенням умов для розумної відкритості і збалансованої розумної закритості для безпечного функціонування суспільства й держави. Світогляд реформаторів у перші роки незалежності держави був пов'язаний з надмірною відкритістю і гласністю, нерозумінням і недооцінкою необхідності охорони таємниць держави та суспільно важливих відкритих інформаційних ресурсів. Руйнування системи режимно-секретних органів та інших спеціальних підрозділів і служб створило передумови для витоку відомостей політичного, економічного, науково-технічного й оборонного характеру. Різні фонди і благодійні зарубіжні організації під гаслом підтримки економічних реформ і вітчизняної науки здійснювали безконтрольне викачування інформаційних ресурсів, особливо пов'язаних із новітніми науковими і технологічними розробками.

Ринкові перетворення і комерціалізація інформаційної сфери торкнулися передусім засобів масової інформації та їх рекламної діяльності. Інформаційні ресурси, що визначають прогресивний соціально-економічний розвиток суспільства і держави, підтримання на необхідному рівні національної безпеки, до сфери ринкових перетворень не включалися. Лише у 1997 році нормативними документами, затвердженими указами Президента України у травні того року, встановлено порядок передавання іншій державі інформації, що становить державну таємницю,

та носіїв такої інформації; у листопаді регламентовано порядок і правила підготовки міжнародних договорів України про взаємну охорону державних таємниць. Указом Президента України «Про заходи щодо охорони інтелектуальної власності в Україні» від 27 квітня 2001 року передбачено розробку і впровадження комплексу організаційних і правових заходів з метою забезпечення прав громадян на захист інтелектуальної власності, сприятливих умов для створення об'єктів інтелектуальної власності, розвитку українського ринку цих об'єктів відповідно до загальноновизнаних світових стандартів.

Однак, незважаючи на вжиті заходи, здійснення міжнародних інформаційних обмінів потребує суттєвого організаційного і правового вдосконалення.

Держава має адекватно реагувати на реалії конкурентної боротьби. Так, за оцінками фахівців щорічні втрати економіки Німеччини від індустріального шпигунства перевищують 40 млрд. марок. За неофіційними даними, втрата торговельних і технічних секретів США обійшлась американським компаніям у 1992 році у 100 млрд. дол. Вважається, якщо не вжити рішучих заходів щодо припинення цих явищ, вказані втрати до 2003 року становитимуть 150 млрд. дол.³⁴⁹. Питання про втрати економіки України з цього приводу — «terra incognita».

У процесі роздержавлення власності, що здійснюється вже тривалий час, оцінка вартості цілісного майнового комплексу об'єкта, що підлягає приватизації, як правило, не враховує вартості фондів науково-технічних бібліотек, наукової й конструкторсько-технологічної документації, а в деяких випадках і об'єктів промислової власності (винаходи, відкриття, промислові зразки, корисні моделі, товарні знаки). Це призвело до того, що значна частина інформаційних ресурсів, яка має комерційну цінність, неправомірно потрапляла до зацікавлених осіб, а державний бюджет внаслідок цього втрачав джерело наповнення. Ці проблеми в повному обсязі залишаються в організаційному і правовому плані не врегульованими і дотепер.

Розглянемо чинники організаційного плану, що негативно впливають на діяльність органів державної влади у сфері управління інформаційними ресурсами України.

В Україні на рівні виконавчої влади відсутній орган, який виконував би функції щодо: розробки стратегії і планування

заходів формування і забезпечення функціонування загальнодержавної системи управління інформаційними ресурсами; безпосереднього організаційного і методичного керівництва міжгалузевими і галузевими структурними елементами цієї системи; розробки і впровадження заходів, спрямованих на комплексне кадрове, фінансове, матеріально-технічне, інформаційне та інші види забезпечення сталого функціонування і подальшого удосконалення системи державного управління інформаційними ресурсами; оцінки результативності дій, витрат бюджетних коштів на забезпечення реалізації державної інформаційної політики, акумуляції досвіду та узагальнення пропозицій міжгалузевих і галузевих елементів системи управління інформаційними ресурсами і підготовки пропозицій для прийняття відповідних політичних і політико-правових рішень на вищому рівні державної влади.

У системі центральних органів виконавчої влади свого часу був створений Державний комітет інформаційної політики, телебачення й радіомовлення, нині — Державний комітет телебачення і радіомовлення, і було б логічним віднести наведені функції до компетенції цього державного органу. Однак ознайомлення із затвердженими функціями комітету та змістом його роботи дає підстави для висновку про те, що він здійснює заходи щодо реалізації державної інформаційної політики лише у сфері діяльності засобів масової інформації (преси), телебачення і радіомовлення та у видавничій сфері. Повноваження щодо проведення аналізу й прогнозування тенденцій розвитку інформаційного простору України та здійснення заходів щодо його захисту також не виходять за межі діяльності засобів масової інформації і видавничої справи.

Відповідно до Указу Президента України «Про Міністерство освіти і науки України» від 7 червня 2000 року це Міністерство в системі центральних органів виконавчої влади забезпечує реалізацію державної політики у сфері освіти, наукової, науково-технічної, інноваційної діяльності і має у своєму складі організаційні структури, що здійснюють реєстрацію й оформлення інформаційних ресурсів науково-технічної інформації (УкрІНТЕІ), здійснюють реєстрацію авторського права, видають охоронні документи на об'єкти інтелектуальної власності та

координують діяльність щодо прав на об'єкти інтелектуальної власності, створені повністю або частково за рахунок коштів державного бюджету.

До компетенції Міністерства освіти і науки віднесено важливу частину діяльності щодо забезпечення реалізації державної інформаційної політики, пов'язаної з державним управлінням інформаційними ресурсами (відкрита наукова, науково-технічна інформація, об'єкти інтелектуальної власності). Однак повноваження і цього Міністерства не поширюються за визначені межі його дії.

Державний комітет зв'язку та інформатизації України відповідно до положення про цей комітет, затвердженого Указом Президента України від 3 червня 2000 року, забезпечує проведення державної політики у галузі зв'язку, розподілу та використання радіочастотного ресурсу та у сфері інформатизації, формує Національну програму інформатизації та забезпечує її виконання.

У сучасних умовах від розвитку галузі зв'язку і телекомунікацій значною мірою залежатиме досягнення головної мети державної інформаційної політики щодо національних інформаційних ресурсів, пов'язаної зі створенням необхідних умов і механізмів формування, розвитку, поширення й ефективного використання інформаційних ресурсів у всіх галузях діяльності, задоволення зростаючих інформаційних потреб особи, суспільства держави. Водночас розвиток галузі зв'язку та телекомунікацій, виконання як Національної програми інформатизації, так і регіональних та місцевих програм і проектів інформатизації здійснюється без урахування необхідності створення загальнодержавної, регіональних і місцевих систем формування електронних баз і банків інформаційних ресурсів, об'єднаних у єдину систему Державної бази метаданих. Державний реєстр інформаційних ресурсів є важливим інструментом державного управління їх формуванням, а повнота метаданих і технологічні механізми поширення забезпечують доступність і задоволення інформаційних потреб громадян, суспільних організацій і державних органів у відкритих інформаційних ресурсах.

Створення системи Державної реєстрації національних інформаційних ресурсів, як це запропоновано в проекті Закону України «Про національні інформаційні ресурси», який погоджу-

вався із зацікавленими державними органами, є проблематичним. Ця проблематичність зумовлена такими аспектами:

- загальнодержавна реєстрація в електронному вигляді повнотекстових інформаційних ресурсів, які створюються в процесі професійної діяльності всієї ієрархічної структури державних органів, підприємств, установ і організацій, з точки зору фінансової, технологічної і просто здорового глузду не тільки неможлива, а й не доцільна;

- у державі на виконання чинного законодавства та відповідних нормативних документів вже створена і діє система формування інформаційних ресурсів за міжвідомчими та відомчими ознаками (науково-технічні, статистичні, правові та інші види інформаційних ресурсів).

За своїм змістом Державний реєстр має бути простим і зручним для користувачів, своєрідним путівником у широкому національному масиві інформації, знань і даних. До Державного реєстру було б доцільним включення сукупності довідково-інформаційних фондів з необхідним довідково-пошуковим апаратом.

Особливого розгляду потребують проблеми державної реєстрації і формування баз і банків даних інформаційних ресурсів, що містять державну таємницю та іншу інформацію з обмеженим доступом як на державному, так і на регіональному та місцевому рівнях. Обіг таких інформаційних ресурсів, їх поширення і використання мають здійснюватися у рамках відповідних режимних заходів, тобто в умовах забезпечення режиму секретності та конфіденційності. Як свідчить світовий досвід, найбільш жорстко охороняється інформація про стратегічні плани забезпечення національної безпеки і оборони та конкретні плани держав щодо їх виконання, а також наукові здобутки, новітні технологічні рішення, ноу-хау, спрямовані на прискорення соціально-економічного розвитку. Така інформація циркулює в інформаційно-телекомунікаційних системах спеціального призначення з впровадженням спеціальних програм доступу і криптографічного захисту та заборобою їхнього виходу на глобальні інформаційні системи.

У сучасних умовах в Україні поки що неможливе формування Державного реєстру інформаційних ресурсів, що містять державну таємницю та іншу інформацію з обмеженим доступом в електронному вигляді, без збитків для суспільства і держави.

Для створення необхідних умов для формування такого реєстру, на нашу думку, доцільно вжити певних заходів, а саме:

- чітко визначити інформаційно-телекомунікаційні системи (ІТС) спеціального призначення, на яких впроваджені відповідні організаційні, програмні, технічні (за необхідності — криптографічні) заходи захисту інформації та які пройшли експертизу в установленому порядку і отримали від спеціально уповноваженого державного органу Атестат на відповідність ІТС для обробки конкретного виду інформації з обмеженим доступом згідно з чинними вимогами;

- у кожному центральному, регіональному і місцевому державному органі у складі підрозділів, що здійснюють державну реєстрацію інформаційних ресурсів і формують бази й банки даних, створити спеціальні служби, укомплектовані кваліфікованими спеціалістами, яким оформлено допуск і надано право доступу до конкретних видів інформації;

- забезпечити спеціальні служби законодавчими, нормативно-правовими актами з питань захисту інформації та розробленими на їх підставі відомчими нормативно-правовими документами (положення, інструкції, методики);

- виділити для роботи спеціальних служб приміщення, в яких гарантовано забезпечується режим секретності (конфіденційності).

Певний досвід правильної організації таких робіт в Україні є. Водночас зазначимо, що державна реєстрація, формування баз і банків даних інформаційних ресурсів в електронному вигляді значно складніші, ніж на паперових носіях, як з точки зору можливостей забезпечення їх гарантованого захисту від витоку, пошкодження й знищення, так і фінансового, і матеріального забезпечення.

Іншим важливим аспектом державної інформаційної політики щодо управління і захисту інформаційних ресурсів є недосконалість структури державних органів, що забезпечують інформаційну безпеку, зокрема, у сфері виготовлення і обігу інформаційних ресурсів.

На даний час на рівні виконавчої влади створені і діють державні органи, які виконують лише частину функцій щодо забезпечення інформаційної безпеки і безпеки у сфері виготовлення і обігу інформаційних ресурсів. Залишається досі не

визначеним державний орган для розробки й упровадження комплексу функціональних заходів забезпечення охорони інформації з обмеженим доступом, що не становить державної таємниці. Організаційно не впорядкована система забезпечення режиму секретності (конфіденційності) у процесі міжнародного інформаційного співробітництва. Режимно-секретні підрозділи і служби у багатьох випадках усуваються від розробки і впровадження цих заходів. Їх здійснення покладається на підрозділи міжнародного співробітництва, спеціалістів, у яких не вистачає знань і досвіду організації режимно-секретного (конфіденційного) забезпечення. Це є однією з причин того, що розвиток міжнародного співробітництва значно випереджає укладання угод із закордонними партнерами про взаємний захист таємної інформації та впровадження інших заходів захисту національних інтересів.

Розглянемо деякі проблеми, пов'язані з діяльністю органів державної виконавчої влади щодо забезпечення інформаційної безпеки і безпеки у сфері виготовлення та обігу інформаційних ресурсів.

У нашій державі офіційно, на рівні законодавчих та інших нормативно-правових актів стосовно інформаційної сфери, функції державних органів розподілені таким чином. Служба безпеки України в сфері забезпечення охорони державної таємниці прогнозує розвиток небезпек, розробляє і здійснює заходи щодо їх упередження, усунення або послаблення їхньої дії. Департамент спеціальних телекомунікаційних систем і захисту інформації Служби безпеки України забезпечує формування, супроводження моделей загроз безпеці інформації в мережах передавання даних та пов'язаних з технічним та криптографічним захистом. Державний комітет телебачення і радіомовлення забезпечує захист інформаційного простору України. Однак у зв'язку з певними організаційними, кадровими, технічними та іншими ресурсними можливостями цей державний орган виконує вказану функцію лише в окремих напрямках.

Значно складнішою є проблема забезпечення інформаційної безпеки та безпеки виготовлення та обігу інформаційних ресурсів. Безумовно, на спеціально уповноважені державні органи мають бути покладені додаткові функції моніторингу всього спектру загроз в інформаційній сфері, розробки і впровадження організаційних, нормативно-методичних заходів, спрямованих

на їх відвертання, усунення або послаблення їхньої дії, оцінки результатів цих дій, витрат на проведення заходів із забезпечення інформаційної безпеки та їх наслідків.

Важливе політичне значення має рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року про створення Міжвідомчої комісії з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України, на яку передбачено покласти функції координації і контролю діяльності за виконанням заходів щодо формування і захисту національного інформаційного простору та забезпечення безпеки в цій сфері, розробки і підготовки проєктів відповідних нормативно-правових документів. Іншими словами, повноваження Міжвідомчої комісії з питань інформаційної політики та інформаційної безпеки передбачено поширити на сферу координації і контролю діяльності органів виконавчої влади, починаючи з вищого органу в системі органів виконавчої влади, яким є Кабінет Міністрів України. Водночас слід зауважити, що Міжвідомча комісія не зможе взяти на себе виконання функцій органів виконавчої влади, компенсувати своєю діяльністю ті ланки виконавчої влади, що не в повному обсязі виконують покладені на них функції, та забезпечити виконання функцій органів виконавчої влади, які ще в організаційному і правовому відношеннях залишаються не визначеними.

Основою створення системи державного управління інформаційними ресурсами є закріплення їх у власності (матеріальній та/або інтелектуальній), забезпечення захисту права власності суб'єктів України, а також правомочностей щодо володіння, користування та розпорядження, які випливають із права власності на інформаційні ресурси.

Проголошених державою у чинному законодавстві прав власності на інформаційні ресурси та прав на об'єкти інтелектуальної власності (патентного, авторського тощо) недостатньо для гарантування передусім прав держави та формування цивілізованого інформаційного ринку, основним дійовим і регулюючим суб'єктом на якому має бути держава. Для розв'язання цих проблем необхідно здійснити комплекс організаційних і правових заходів.

Розглянемо найбільш важливі аспекти організаційних заходів, що випливають із права власності держави на інформаційні

ресурси, створені на кошти державного бюджету, позабюджетних фондів та інших надходжень із коштів платників податків.

Перший аспект. В Україні створена і діє система обліку державного майна та нерухомості. Функції реалізації державної політики у цій сфері здійснює Фонд державного майна України, в тому числі й пов'язані з приватизацією, тобто роздержавленням власності. Систему державного обліку інформаційних ресурсів як майна або нематеріальних активів не створено. Основні масиви інформаційних ресурсів, з точки зору організаційної та правової, знеособлені. Виняток становлять лише окремі види інформаційних ресурсів, що охороняються патентами та відповідними свідоцтвами. Однак і цей варіант захисту права власності не завжди поширюється на захист права власності держави. Отже, важливим аспектом цієї проблеми є створення системи обліку інформаційних ресурсів, створених повністю або частково за рахунок державних коштів і визначення державного органу, що здійснював би державну політику в цій сфері діяльності. Таким державним органом можуть бути Фонд державного майна України та його регіональні підрозділи.

Другий аспект. У зв'язку з тим, що роздержавлення власності триває більше десяти років, створення системи обліку державних інформаційних ресурсів є складною проблемою, особливо у питанні відновлення необґрунтовано втрачених прав держави на інформаційні ресурси в процесі приватизації (конструкторсько-технологічна документація, винаходи, відкриття, промислові зразки, корисні моделі та ін.).

Можливим варіантом розв'язання цієї проблеми є проведення інвентаризації інформаційних ресурсів за участю представників Фонду державного майна України, міністерств, відомств, до сфери управління яких належать підприємства, установи та організації, в тому числі й ті з них, що вже приватизовані, а також представників інших зацікавлених центральних державних органів та органів місцевого самоврядування і відповідних державних адміністрацій. Підставою для проведення такої інвентаризації має бути рішення Кабінету Міністрів України, яке встановило б порядок, правила і строки її проведення, форму звітності.

Результатом інвентаризації має бути включення державних інформаційних ресурсів як майна або нематеріальних активів

до складу основних фондів підприємств, установ, організацій. У разі порушення права власності держави на інформаційні ресурси, створені на державні кошти, відновлення цих прав доцільно вирішувати в порядку, встановленому законодавством. Надалі на порядок, правила і строки проведення інвентаризації державних інформаційних ресурсів доцільно поширити вимоги, що регламентують проведення інвентаризації державного майна.

Глибоко помиляються ті представники наукової та управлінської еліти, які роблять спроби створити державну систему управління державними інформаційними ресурсами та захисту прав держави в цій сфері без формування системи обліку інформаційних ресурсів як майна та нематеріальних активів. Облік державних інформаційних ресурсів як активів забезпечуватиме: гарантії їх збереження та ефективність використання з дотриманням державних інтересів; проведення свідомої цілеспрямованої фінансово-економічної політики щодо формування державних інформаційних ресурсів та їх комерційного та некомерційного використання; страхування ризиків, пов'язаних із використанням інформаційних ресурсів; вирішення питань поповнення державного бюджету, що особливо важливо в сучасних умовах.

Третій аспект. Важливим аспектом державної політики щодо управління і захисту інформаційних ресурсів є впорядкування системи фінансування заходів, пов'язаних із формуванням, поширенням, використанням і захистом інформаційних ресурсів. Усунути проблеми, пов'язані з фінансуванням робіт за залишковим принципом у цій сфері діяльності, без чіткого закріплення цих функцій за головним фінансовим органом держави, яким є Міністерство фінансів, є досить проблематичним. Функції цього державного органу виконавчої влади можуть бути викладені в такій редакції: „Здійснення державної політики щодо фінансування системи формування і захисту державних інформаційних ресурсів, забезпечення їх комерційного і некомерційного використання та розвитку інформаційного ринку».

Четвертий аспект. Принциповим питанням державної інформаційної політики щодо управління і захисту інформаційних ресурсів України є створення умов для нарощування вітчизняного потенціалу інформаційних і телекомунікаційних технологій

та управління з боку держави цими процесами. Інформаційно-телекомунікаційні технології є системоутворюючим елементом інформаційного простору, який визначає рівень формування, поширення, використання інформації як ресурсу та забезпечує його захист. В умовах, коли ринок України захоплено світовими виробниками цієї продукції, тільки констатуванням, заклинами та безсистемним розвитком електронного та інших, пов'язаних із цим напрямом виробництв, розв'язати ці проблеми неможливо.

Відповідно до висновків³⁵⁰, саме нові інформаційні технології забезпечують різке підвищення продуктивності у ключових галузях промисловості, сфері послуг та ін., що за рахунок електронного маркетингу і менеджменту собівартість продукції в розвинутих країнах зменшилась на 10 — 12%, а зростання продуктивності праці становить понад 30 — 40%. Водночас «відсталі» країни (які розвиваються, та ті, що не приділяють належної уваги розвитку інформаційних технологій), поступово опиняються дедалі в більшій залежності від «лідерів» у галузі нових технологій. На думку автора, у недалекому майбутньому воєнну та ортодоксальну економічну експансію великих держав у світі має замінити «інформаційно-технологічний колоніалізм».

Створення умов для нарощування вітчизняного потенціалу інформаційно-телекомунікаційних технологій та їх ефективного використання в інтересах суспільства і держави, з урахуванням світового досвіду, погляду на цю проблему вітчизняних та зарубіжних учених, має включати вирішення таких питань:

- чітке визначення напрямів державної політики щодо управління процесами розробки, виробництва і практичного застосування вітчизняних інформаційно-телекомунікаційних технологій та покладання функцій з координації та контролю цієї діяльності на державний орган виконавчої влади;

- зосередження на цьому напрямі діяльності держави досвідчених вітчизняних учених і висококваліфікованих спеціалістів з одночасною підготовкою кадрів для сфери розробки, виробництва і практичного застосування інформаційно-телекомунікаційних технологій у різних галузях життєдіяльності суспільства і держави;

- включення до класифікатора економічної діяльності нової галузі економіки під назвою «Виробництво інформаційних, те-

лекомунікаційних технологій і послуг» із покладанням відповідних функцій щодо реалізації державної економічної політики у цій галузі на Міністерство економіки та з питань європейської інтеграції України.

П'ятий аспект. Стале функціонування системи управління і захисту інформаційних ресурсів України та інформаційної безпеки безпосередньо залежить від кадрового забезпечення професійно підготовленими спеціалістами та рівня інформаційної культури суспільства.

Важливе значення для удосконалення системи підготовки кадрів у цій сфері діяльності мають рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року за результатами розгляду питання «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України», якими передбачено: впровадження комплексу заходів щодо підготовки та перепідготовки спеціалістів у сфері інформаційної безпеки; розробки типових навчальних програм для середніх та вищих навчальних закладів з навчальної дисципліни «Інформаційна культура»; вжиття заходів підвищення рівня підготовки управлінських, журналістських та технічних кадрів для інформаційної сфери, в тому числі працівників державних органів, врахування сучасних потреб при формуванні державного замовлення на підготовку молодих фахівців. Це важливі стратегічні завдання щодо розв'язання проблем підготовки суспільства і держави, державних інституцій для забезпечення вдосконалення управління інформаційною сферою, ефективного використання інформаційних ресурсів — важливого національного надбання та ресурсної складової захисту національних інтересів в інформаційній сфері. Для виконання цих завдань потрібно кілька років цілеспрямованої праці.

Водночас доцільно підкреслити, що формування логічно завершені системи управління і захисту інформаційних ресурсів треба було розпочинати ще вчора, тобто забезпечувати виконання законодавчих і нормативно-правових актів та інших заходів загальнодержавного значення будуть керівники і спеціалісти, якими укомплектовані сьогодні центральні, регіональні і місцеві державні органи, їхні спеціальні підрозділи і служби. У зв'язку з цим для забезпечення єдиних підходів щодо реалізації державної політики у сфері управління інформаційними

ресурсами і забезпечення безпеки сфери їх виготовлення та обігу, було б доцільно провести спеціальну державну атестацію керівників усіх рівнів та спеціалістів, на яких покладено обов'язки щодо розробки і впровадження заходів забезпечення реалізації державної політики у сфері їх відання, на предмет відповідності посадам, які вони обіймають. Критерії для проведення такої атестації доцільно розробити спеціально уповноваженими державними органами, що здійснюють управління конкретними напрямками інформаційної сфери та захистом інформаційних ресурсів, погодити процедуру атестації з Головердержслужбою і затвердити Урядом України.

Актуальною проблемою, яка має важливе загальнодержавне значення, є необхідність підвищення інформаційно-правової культури суспільства (правосвідомості), спрямованої на усвідомлення і розуміння кожним громадянином: своїх прав на інформацію та свободу інформаційної діяльності; своїх обов'язків щодо інформаційної безпеки та захисту інформації; обмежень прав на поширення інформації, що встановлює держава в інтересах національної безпеки, іншої суспільної необхідності, захисту життя, здоров'я та гідності людини.

Як зазначалося³⁵¹, свобода — це не всюдозволеність і безконтрольність, має бути баланс відкритості та обмеження свободи одержання і використання інформації, якщо це йде на шкоду іншим людям, державі, суспільству в цілому, і особливої уваги заслуговують проблеми ЗМІ як поширювачів масової інформації. На думку автора, в сфері ЗМІ потрібен баланс: з одного боку, свобода, відсутність державної цензури, з іншого — громадський і державний контроль за недопущенням зловживань свободою преси, інших засобів масової інформації.

Законодавства розвинутих країн щодо свободи інформаційної діяльності передбачають спеціальні норми про підстави обмеження відкритого доступу до певних видів закритої інформації та відповідальності за порушення цих правових норм.

Боротьба за свободу думки, слова, а згодом і преси сягає у далеке історичне минуле. Зі стародавніх часів вживаються заходи щодо обмежень інформаційних свобод. У цьому плані велику цінність має праця І. В. Мусієнка³⁵². Боротьба цих двох напрямів відповідно до ґрунтовних висновків автора пов'язана з

тим, що свобода слова (преси) може бути спрямована як на благо, так і на шкоду особистості і суспільству.

На основі аналізу законів про пресу Німеччини, Франції, Великої Британії, Росії (кінець XIX — початок XX століть) та історії боротьби за свободу слова і преси між суспільством і правлячими класами, І. В. Мусієнко простежує еволюцію законодавства з цих питань, починаючи з римського права. Відповідно до свідчень автора з XVI століття всі держави Західної Європи вводять цензуру. Ідея свободи слова найраніше закріплюється — в Законі про пресу в Англії, однак цей закон містить норми про відповідальність за необережність у пресі. Згодом такі норми були введені у німецькому та російському законодавстві. Відповідальність за необережність у пресі поширювалася на відповідального редактора періодичного видання і видавця неперіодичного видання за публікацію матеріалів, які підбурюють до антисуспільних, антидержавних дій³⁵³.

Сучасні закони про свободу слова та право на інформацію у США, Великій Британії, Німеччині, Франції та інших державах також містять спеціальні правові норми про підстави для обмеження доступу до певних видів інформації. Завдяки стабільно існуючій системі формування правовосвідомості суспільств, обмеження з боку держави свободи слова та права на інформацію сприймається як суспільна необхідність.

В Україні реалізацію права на інформацію та свободу інформаційної діяльності з додержанням установлених на рівні законів вимог режиму секретності та конфіденційності ділових інформаційних відносин доцільно розглядати як важливий показник оцінки громадської, професійної культури державного службовця, науковця, журналіста, підприємця, спеціаліста та інших громадян — учасників суспільних інформаційних відносин. Цей показник має стати нормою суспільного життя. Для цього доцільно впровадити комплекс правових, освітніх, організаційних заходів.

Попри значущість впливу зовнішніх чинників на формування іміджу України, ключовим і визначальним фактором його формування залишається рівень поінформованості світової громадськості про внутрішньополітичні та соціально-економічні процеси в державі. Інформація про подальші позитивні внутрішні зміни може поліпшити імідж України в світі лише за умови добре

скоординованих зовнішньополітичних зусиль і застосування державою цілеспрямованих «PR-технологій» (PR — це ефективно працююча наука та мистецтво досягнення взаєморозуміння та згоди між різними суб'єктами життя громадянського суспільства)³⁵⁴.

Однією з передумов існування та функціонування держави є інформаційний обмін. Системи, організовані з розподілом праці, не могли б функціонувати без обміну інформацією³⁵⁵.

Інформація відіграє роль спілкування як між суспільними групами, так і між державами.

Координуюча та вирішальна роль у визначенні й реалізації практичних форм організації інформаційних зв'язків України з іншими країнами світу належить органам державного управління.

Кожна владна структура створює потоки інформації, через які впливає на суспільну свідомість, в тому числі на формування іміджу своєї держави у світі. Визначальною рисою таких інформаційних потоків є їх зворотність. Основні, базові складові типової моделі таких інформаційних потоків у зовнішньополітичній сфері мають такий вигляд. Між суб'єктом (держава через органи державного управління) та об'єктом (дипломатичні представництва України і неурядові структури за кордоном) відбувається двосторонній інформаційний обмін. Від суб'єкта до об'єкта йде низхідна інформація — розпорядження, директивні та регламентуючі матеріали, плани, конкретні вказівки тощо. Назад повертається висхідна зворотна інформація, яка, зокрема, може бути проінтерпольована з точки зору стану і тенденцій змін в іміджі держави на терені міжнародних відносин. Крім вертикальних інформаційних зв'язків, існують горизонтальні, які мають велике значення у координації роботи між підрозділами, не пов'язаними відносинами підлеглості.

Таким чином, на базі діючих механізмів зворотного зв'язку в Україні сформовано передумови для впровадження ефективної системи оперативного державного реагування на зміни в іміджі.

Інформаційно-аналітичний внесок урядових структур у створення міжнародного іміджу держави полягає в організації роботи по створенню об'єктивної інформації щодо всіх аспектів своєї політики, діяльності, результатів впровадження програм та

проектів. Така інформація має бути повною, об'єктивною, зрозумілою, надходити своєчасно і бути доступною. Міжнародній спільноті також принципово важливо знати відповідність національних пріоритетів соціально-економічного розвитку сучасним цивілізованим нормам і стандартам громадянського суспільства. Основою для формування позитивного іміджу України є насамперед внутрішньополітична стабільність, прогресивний розвиток економіки, реформування українського суспільства, європейський вектор зовнішньої політики та зміцнення місця і ролі України у світі³⁵⁶.

На думку автора, можна визначити такі функції інформаційного управління у сфері формування іміджу держави: виявлення цілей і постановка (загальних і конкретних); підготовка пропозицій для прийняття рішень; прийняття рішень та їх реалізація; оцінка досягнутих результатів; опрацювання і вжиття коригуючих заходів.

Формування і здійснення збалансованої державної політики, спрямованої на позитивне сприйняття України у світі, невід'ємне від ефективного проведення комплексу узгоджених заходів щодо захисту національних інтересів у політичній, економічній, соціальній, військовій, екологічній, науково-технічній, інформаційній та інших сферах національної безпеки (комплекс характеристик, який у попередньому пункті даної роботи умовно названо «стартовими» умовами).

Важливою складовою розробки та проведення вищезазначеної політики є чітке дотримання норм системи забезпечення національної безпеки, що являє собою організовану державою сукупність суб'єктів: державних органів, громадських організацій, посадових осіб та окремих громадян, об'єднаних цілями та завданнями щодо захисту національних інтересів.

Однією з основних функцій системи забезпечення національної безпеки є участь у міжнародних системах безпеки, а також створення і підтримка в готовності сил та засобів забезпечення національної безпеки³⁵⁷.

Зовнішня політика держави як суб'єкта міжнародного права визначає не тільки характер міжнародних відносин, а й в сучасних умовах має безпосередній вплив на суспільну і соціально-психологічну свідомість, ступінь свободи та рівень благополуччя громадян на національному рівні. У сфері зовнішньої

політики можна виділити кілька основних напрямів забезпечення інформаційної безпеки держави:

- розробка державної політики у сфері удосконалення інформаційного забезпечення зовнішньополітичного курсу країни;

- розробка та реалізація комплексу заходів щодо посилення безпеки інформаційної інфраструктури органів виконавчої влади, які причетні до питань реалізації зовнішньої політики держави;

- надання українським представництвам та організаціям за кордоном повноважень щодо здійснення активних інформаційних заходів з питань нейтралізації поширюваної там дезінформації про зовнішню і внутрішню політику України.

Отже, в умовах інформаційного суспільства особливої уваги потребує вирішення державними органами питання безпечного функціонування інформаційної сфери як визначального фактору, що впливає на формування позитивних тенденцій у розвитку міжнародного іміджу держави.

Таким чином, незважаючи на те, що в державі створена певна система організаційного забезпечення формування і реалізації державної інформаційної політики управління і захисту інформаційних ресурсів, ця система потребує суттєвої оптимізації структури державних органів, що реалізують державну інформаційну політику, забезпечення чіткого визначення і розмежування їхніх повноважень, налагодження між ними ефективної взаємодії і координації, а також контролю за їхньою діяльністю, створення ефективно діючих організаційних структур забезпечення інформаційної безпеки, в тому числі у сфері виготовлення й обігу інформаційних ресурсів. Успішно вирішити ці питання можна, лише керуючись об'єктивними закономірностями, що діють в інформаційній сфері та сфері управлінської діяльності і передбачають визначення, на підставі головної мети, функції державного управління і захисту інформаційних ресурсів, створення для їх виконання відповідної ієрархічної організаційної структури державних органів, їхніх спеціальних підрозділів і служб.

Водночас Державний бюджет України передбачає фінансування розвитку інформаційної сфери лише за окремими статтями витрат (державне телебачення і радіомовлення, інформатизація, частково забезпечення інформаційної безпеки). Сфера

формування інформаційних ресурсів та забезпечення інформаційних потреб громадян, суспільства і держави на безприбутковій основі та на доходи від комерційного використання державних інформаційних ресурсів, а також у повному обсязі сфера забезпечення інформаційної безпеки залишаються поза увагою розробників проекту Державного бюджету України і законодавців.

Аналогічно до Державного бюджету України формуються і статті витрат на розвиток інформаційної сфери у регіональних і місцевих бюджетах.

Програма діяльності Кабінету Міністрів України «Реформи заради добробуту», затверджена Верховною Радою України, також не приділяє пріоритетної уваги удосконаленню системи державного управління й захисту інформаційних ресурсів України. У цьому важливому державному документі положення про захист інформаційної сфери зведено до вдосконалення системи фінансування державного телебачення, а основні напрями діяльності уряду щодо розвитку національного сегмента Інтернету — до розробки Концепції пріоритетного розвитку Інтернету в Україні. Необхідність адекватної оцінки і розв'язання зазначених проблем зумовлено тим, що:

- у сучасних умовах значно розширилися можливості для реалізації конституційних прав громадян на інформацію та свободу інформаційної діяльності, суттєво зросли потреби потенційно активної частини суспільства в інформаційній взаємодії як усередині країни, так і за її межами;

- інтенсивний розвиток глобальної інформаційної інфраструктури, необхідність інтеграції України у світове інформаційне співтовариство на рівноправних умовах посилили залежність ефективного функціонування суспільства і держави від стану розвитку інформаційної сфери, передусім системи державного управління національними інформаційними ресурсами;

- інформаційні ресурси, інформаційна інфраструктура в сучасних умовах стають ареною міжнародної боротьби за світове лідерство, за досягнення певних стратегічних і тактичних політичних цілей. І, що необхідно підкреслити особливо, володіння інформацією, належне інформаційне забезпечення органів державного управління є основою успішної боротьби із сучасним тероризмом;

— інформаційна революція перетворилася на революцію у війсьній справі — вона надала можливості вивести з відчутної сфери, *віртуалізувати* багато складових війни: як мінімум, передвоєнний період, підготовку до нанесення удару без звичайного загрозливого періоду, а в деяких випадках і всю війсьну кампанію провести у віртуальному варіанті. Водночас, незважаючи на віртуальність ведення війни тільки в інформаційних мережах і системах обробки інформації, можна, не залучивши жодного солдата, здійснити заходи, наслідком яких буде повне підкорення економіки і політики супротивника.

* *
*

Розвиток соціальних систем відбувається шляхом розвитку і вдосконалення інституцій, які і персоніфікують національні економіки. Знання особливостей інституційної розбудови системи формування і використання змістовного інформаційного ресурсу підвищує ефективність розвитку соціальної системи та ступінь передбачуваності такого розвитку.

За світовим досвідом, формування ЗІР та його використання здійснюється на чітко визначених правових і організаційних засадах щодо науково-технічних досліджень, науково-технічної статистики, прогнозування, оцінки наукового і технічного рівня отриманих здобутків. Державна політика стосовно формування і використання ЗІР може бути реалізована відповідними правовими механізмами та активними заходами органів управління міжгалузевого, галузевого та ієрархічного рівня, оскільки процес концентрування ЗІР прямо залежатиме від інноваційно-інвестиційної політики держави. Для сучасної організації інформаційної складової науково-технічної діяльності стала характерною адаптація понять та принципів науки про управління, що виникла у США. Такі терміни, як оцінка, моніторинг, менеджмент тощо останні 20 — 30 років активно прижилися у сфері науки та політики, спрямованої, зокрема, на управління процесами формування і використання ЗІР за науково-технічними здобутками держави.

Формування ЗІР за науково-технічним доробком країни, його використання не тільки з метою отримання знання, а й для

управління наукою, виробництвом, фінансовою сферою, маркетинговою діяльністю потребує удосконалення управління інформаційними ресурсами функціонального характеру, що має відбиватися у державній інформаційній політиці.

Інституційна складова державної політики формування і використання ЗІР дає змогу послідовно здійснювати комерціалізацію науково-технічних досягнень, забезпечення охорони інтелектуальної власності, інформаційного забезпечення популяризації наукових здобутків як у вітчизняному господарстві, так і у сфері міжнародного науково-технічного співробітництва.

Державна інформаційна політика та стратегія управління національними інформаційними ресурсами має передбачати:

— формування ринку інформаційних продуктів і послуг шляхом застосування антимонопольних заходів, формування необхідного наукового, матеріально-технічного, фінансового і трудового потенціалу виробництва ІПП, у тому числі тих, які не становлять комерційного інтересу, але є важливими для розвитку господарства у цілому, а також для інноваційно-інвестиційної політики, встановлення пріоритетів науково-технічного та економічного розвитку держави;

— удосконалення наявної інформаційної інфраструктури, її організаційно-правових засад, створення відповідних функціонально-структурних ланок, розвиток вітчизняної бази інформаційно-телекомунікаційних технологій для інформаційної діяльності у науково-технічній сфері, системі охорони об'єктів інтелектуальної власності при здійсненні трансферу технологій;

— впровадження організаційних (за вертикаллю) умов для здійснення управлінських заходів стосовно створення загальної системи захисту інформаційних ресурсів з обмеженим доступом та відкритої інформації, важливої для суспільства і держави. Цей напрям доцільно розглядати як пріоритетний та виокремити в системі національної безпеки як самостійну сферу діяльності.

Інформаційна безпека як стан захищеності життєво важливих інтересів особи, суспільства і держави в інформаційній сфері охоплює систему політичних, економічних, правових, організаційних, наукових, інформаційних тощо заходів, спрямованих на виявлення, запобігання або нейтралізацію реальних та потенційних загроз, що діють у цій сфері.

Як свідчить світова практика, найбільше охороняються серед інформаційних ресурсів — ЗІР за науково-технічним до-робком. Кожна держава вживає певних заходів для захисту національних інтересів у сфері науково-технічної інформації, що визначає прогрес економічного і соціального розвитку, стає функціонування систем національної безпеки. При цьому слід враховувати як внутрішні чинники, пов'язані із забезпеченням балансу інтересів особи, суспільства, держави, так і зовнішні — щодо адаптованості інформаційної сфери до глобалізаційних процесів.

Удосконалення системи державного управління і захисту інформаційних ресурсів залежатиме від визначення державною інформаційною політикою її цілей стосовно СНІР, державно-управлінських функцій щодо їх досягнення та оптимальної структури державних органів для виконання цих функцій.

В Україні сформована і функціонує відомча система щодо СНІР, загальнодержавна система охорони державної таємниці та захисту інформації в мережах передавання даних, технічного і криптографічного захисту інформації. Водночас залишається неформованою загальнодержавна система управління і захисту інформаційних ресурсів, не об'єднані єдиною метою та завданнями державні органи, що входять до цієї структури.

На вищому стратегічному рівні потребує вдосконалення координація правотворчого процесу щодо формування правових засад побудови, забезпечення функціонування і розвитку системи управління і захисту інформаційних ресурсів. На рівні органів державної виконавчої влади доцільно оптимізувати державно-управлінські функції та створити ієрархічну вертикаль формування, поширення, використання і захисту інформаційних ресурсів. Стосовно державної таємниці може йтися про вдосконалення цієї системи, стосовно ж іншої інформації з обмеженим доступом — необхідно розробити і впровадити правові та організаційні механізми її функціонування. Важливими аспектами державно-управлінської діяльності у сфері СНІР є закріплення їх у власності, створення державної системи реєстрації ІР, нарощування вітчизняного потенціалу інформаційно-телекомунікаційних технологій, кадрового забезпечення та підвищення інформаційної культури суспільства.

Розділ 4

ЗАХИСТ ІНФОРМАЦІЇ - ПРІОРИТЕТНЕ ЗАВДАННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Захист таємниць супроводжує людство на всіх етапах розвитку цивілізації. У країнах, які оцінюються як еталон демократії, захищеність національних інтересів в інформаційній сфері — пріоритетного завдання національної безпеки — завжди належала до найвищих національних цінностей, що мають, без перебільшення, не менше значення, ніж свобода слова. Особливої актуальності вона набуває після відомих терористичних актів у різних регіонах світу.

Розв'язання цих проблем — на шляху формування виваженої державної інформаційної політики та інформаційної безпеки України, яка має реалізовуватися відповідними правовими актами та організаційними заходами держави.

4.1. Історія формування державної системи захисту інформації

Після розпаду СРСР у нашій державі від колишньої системи захисту інформації залишилася лише нижча ланка (режимно-секретні органи, підрозділи протидії іноземним технічним розвідкам) на підприємствах, установах і в організаціях. Нормативно-правовою базою захисту інформації були підзаконні акти. У сфері охорони державної таємниці діяв Перелік найголовніших відомостей, що становлять державну таємницю СРСР, розроблений у надрах «НКВД — МДБ — КДБ», та інструкції з грифами секретності. За погодженням із КДБ СРСР розроблялися відомчі переліки відомостей, віднесених до державної таємниці СРСР. Ці документи передбачали тотальну засекреченість не

тільки найважливіших сфер діяльності суспільства і держави, а й підприємств, установ, міст та цілих регіонів. Організація, координація діяльності у сфері охорони державної таємниці та широкі повноваження щодо контролю за її станом були покладені на КДБ СРСР.

Як зазначалося, в 70—80-х роках минулого століття провідні країни світу започаткували широкомасштабне впровадження і застосування технічних засобів розвідки, які, за оцінками різних експертів, постачали до 70% доброякісної розвідувальної інформації. Протидія технічним розвідкам у СРСР стала завданням державної важливості і однією із складових частин у загальній системі заходів для забезпечення державної і службової (військової) таємниць. Концептуальні, організаційні, науково-технологічні і нормативні основи протидії технічним розвідкам не втратили наукового і практичного значення і використовуються державною владою країн СНД.

Так, Російською Федерацією прийнято ряд важливих принципів рішень, зокрема, на базі Держтехкомісії СРСР Указом Президента Росії у січні 1992 року було утворено Державну технічну комісію при Президентові РФ як орган державного управління, а після прийняття Закону Російської Федерації «Про державну таємницю» утворено Міжвідомчу комісію з захисту державної таємниці. Створення міжвідомчих колегіальних органів державного управління у сфері захисту інформації, безпосередньо підпорядкованих Президенту Росії, забезпечило максимальне врахування передусім суспільних інтересів, умови для унеможливлення монополізму в процесі прийняття державних рішень, дало змогу зробити вихід на якісно новий рівень розвитку державної системи захисту інформації в Російській Федерації.

Слід зазначити, що з розпадом СРСР загальнодержавні організаційні, координаційні і науково-методичні органи і центри залишилися у Російській Федерації.

Автору даної монографії протягом 1993—1999 років довелося бути безпосереднім учасником процесів формування і становлення системи захисту інформації в Україні, працюючи на посадах заступника двох голів Державної служби України з питань технічного захисту інформації Л. В. Деркача і Ю. О. Семенова і єдиного Державного комітету України з питань державних

секретів та технічного захисту інформації П. О. Мисника і цією роботою мені хотілося б вшанувати наполегливу роботу першої плеяди керівників уряду, зокрема В. П. Пустовойтенка, фахівців, які спромоглися в стислі строки на хорошому рівні виконати значний обсяг науково-організаційної роботи, випередити на тому етапі всі суверенні країни СНД, включаючи Росію, у створенні нормативно-правової бази системи захисту державної таємниці та ТЗІ і закладання основ її функціонування.

Сьогодні доцільно нагадати про те, що на початку 1990-х років якісні зміни у військово-політичній і соціально-економічній сферах змусили незалежні держави, що утворилися на теренах колишнього СРСР, переглянути державну політику в галузі захисту інформації, отримати законодавче закріплення свободи слова, право на свободу інформаційної діяльності; припинити існування державної монополії на інформаційні ресурси. Закінчення воєнно-політичної конфронтації, розвиток довіри у військовій сфері вимагали від молодих незалежних держав поєднання розумної відкритості і заходів захисту власних таємниць, існуюча ж як спадщина від СРСР нормативно-правова база заважала будівництву демократичних держав. Застосування колишніх адміністративних методів управління захистом інформації стало неможливим і неефективним, оскільки обмеження прав на інформацію мало бути врегульоване виключно законами.

Система захисту інформації, яка залишилася у спадщину, гальмувала розвиток міжнародних відносин України, розширення міждержавного економічного, науково-технічного, культурного, гуманітарного тощо співробітництва вимагали нових підходів до віднесення відомостей до таємниць держави та застосування режимно-секретних обмежень.

Крім того, розвиток інформаційно-телекомунікаційних систем, застосування інформаційних технологій внесли докорінні зміни в погляди і підходи до визначення обсягів інформації, що підлягає охороні, принципів, методів і засобів її захисту.

Однак першопричиною необхідності реформування системи захисту інформації слід вважати зміну економічного базису суспільства, яка безпосередньо вплинула на трансформації його політичної надбудови. Якщо із сукупності всієї інформації виділити закриту інформацію і порівняти співвідношення між сек-

ретами виробництва (так званими ноу-хау), комерційною таємницею та державною таємницею за станом на 1991 і 2001 роки, то графічно їх обсяги можна подати таким чином (у даному випадку для нас важливі не так кількісні, як якісні характеристики) (рис. 6).

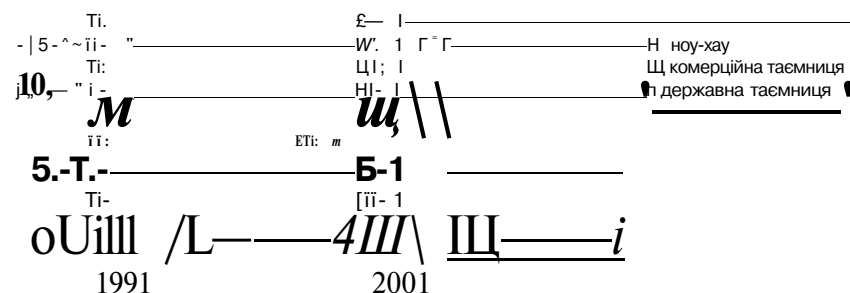


Рис. 6. Умовне співвідношення інформації ноу-хау, комерційної таємниці і державної таємниці у підмножині закритої інформації, тобто інформації, яка потребує захисту в різних соціально-економічних умовах

Отже, при відносному зменшенні обсягів інформації, віднесеної до державної таємниці, в нових соціально-економічних умовах значно зростають обсяги інформації, віднесеної до інформації ноу-хау (секрети виробництва) і комерційної таємниці. До того ж слід враховувати, що відсутня чітка управлінська вертикаль, яка існувала за попередньої соціально-економічної системи, в нових соціально-економічних умовах, які характеризуються різноманіттям форм власності, приватизовані або акціоновані підприємства випадають з підпорядкованості міністерств і відомств, і навіть методичне керівництво ними з питань захисту інформації стає проблематичним.

Процес цей триватиме, оскільки на даний час, як зазначив у своєму інтерв'ю газеті «Урядовий кур'єр» (5 червня 2003 р.) дер-

жавний секретар Міністерства промислової політики України В. Падалка, майже повністю приватизовані металургійна галузь, легка, деревообробна, меблева промисловість, змінили форму власності 80 % машинобудівних підприємств, водночас Програмою приватизації передбачено поглиблення процесу приватизації в Україні й у найближчій перспективі планується залучити до нього літакобудування та суднобудування, додамо від себе — галузі промисловості, в яких традиційно концентрувалася закрита інформація. Таким є головний фактор, який необхідно врахувати при створенні системи захисту інформації в Україні.

Іншим проблемним питанням щодо захисту інформації, насамперед державної таємниці, стала поява в керівництві підприємств, установ і організацій іноземних громадян.

За таких умов з набуттям незалежності почалося становлення системи захисту інформації в Україні. Можна вважати, що перший етап завершується прийняттям Закону України «Про державну таємницю» від 21 січня 1994 року і Положення про технічний захист інформації в Україні (постанова КМ України від 9 вересня 1994 року), які створили правову основу охорони державної таємниці молодій незалежній державі з урахуванням власного досвіду і досвіду розвинутих демократичних країн.

Після проголошення незалежності України Верховною Радою України приймається Постанова «Про порядок тимчасової дії на території України окремих актів законодавства Союзу РСР» від 12 вересня 1991 року. Цією постановою передбачалося, що до прийняття відповідних актів законодавства України на території країни застосовуються акти законодавства СРСР з питань, які не врегульовані законодавством України і якщо вони не суперечать Конституції і законам України. Однак часові і кваліфікаційні обмеження працівників державної влади того часу залишили чинними значну кількість нормативних підзаконних актів СРСР у сфері охорони державної, службової і військової таємниць та технічного захисту інформації, багато з яких суперечили основам демократичної правової держави.

Слід нагадати, що з розпадом СРСР загальнодержавні органи, які здійснювали науково-організаційну та координаційну діяльність у сфері захисту інформації, а також науково-методичні центри, залишилися на території Росії. На органи КДБ

УРСР були покладені лише функції оперативно-розшукового забезпечення захисту інформації з обмеженим доступом, проведення спеціальних перевірок громадян у зв'язку із допуском до державної таємниці, криптографічний захист інформації та досудового слідства щодо злочинів, пов'язаних з державною таємницею.

До того ж, як вважав тоді законодавець, у демократичному суспільстві не доцільно було зосереджувати у спеціальному правоохоронному органі, яким є Служба безпеки, спеціальні функції і нормативно-методичне забезпечення, координацію і контроль охорони державної таємниці, оскільки зосередження наведених функцій в Службі безпеки України створюватиме умови для порушення прав і свобод людини з боку спецслужб. Аргументом була необхідність посилення цивільного контролю за сферою обмеження прав на інформацію і забезпечення свободи слова. Законами України «Про Службу безпеки України» і «Про оперативно-розшукову діяльність» на СБУ поклалися лише спеціальні функції (оперативно-розшукове забезпечення, проведення спеціальних перевірок громадян у зв'язку із допуском до державної таємниці, криптографічний захист інформації та досудове слідство щодо злочинів у сфері державної таємниці). Тобто вона фактично позбавлялася права здійснювати контроль за станом охорони державної таємниці навіть в інтересах виконання, покладених на цей орган спеціальних функцій.

Під час розгляду проектів законів, які мали регламентувати діяльність Служби безпеки України, Верховна Рада України підтримала пропозиції щодо створення в системі державного управління органів державної виконавчої влади із завданнями і функціями забезпечення захисту інформації. Рішення про створення таких структур у системі центральної виконавчої влади були прийняті у першому півріччі 1993 року.

Ті два роки (кінець 1991 — до кінця 1993 року) були найбільш важкими для системи захисту інформації, яка існувала, оскільки на підприємствах, в установах, організаціях, в державних органах були накопичені великі обсяги документації, промислових об'єктів, спецвиробів, обладнання, які містили інформацію з обмеженим доступом (державну, службову і військові таємниці). Водночас за відсутністю з боку держави організації, координації і контролю у сфері захисту інформації здійснювалося

стихийне формування системи державного управління цією сферою діяльності, а в багатьох випадках активно руйнувалася колишня система. У той період в Україні фактично залишилися залишки старої системи захисту інформації, а суб'єкт управління процесом формування в державі нової системи захисту інформації на державному рівні не був визначений, відповідно в органах державної виконавчої влади втрачався кадровий потенціал, а фінансові ресурси для формування системи захисту інформації не передбачалися.

Так, у Міністерстві машинобудування, промислової політики і конверсії України, яке утворилося на базі дев'яти міністерств і семи державних комітетів, був сформований режимно-секретний орган у кількості трьох посадових осіб, підрозділу протидії іноземним технічним розвідкам для організації і координації технічного захисту інформації не було. Міністерство зовнішніх економічних зв'язків і торгівлі, утворене на базі двох міністерств, сформувало режимно-секретний орган у складі двох спеціалістів, підрозділи з питань технічного захисту інформації були ліквідовані.

За оцінками експертів, до середини 1993 року в Україні чисельність режимно-секретних органів та спеціальних підрозділів і служб з питань технічного захисту інформації скоротилася більш як у 100 разів. Тобто керівництво країни було позбавлене інструменту для відповідного контролю і координації за діяльністю науково-промислового комплексу.

Перші кроки незалежності держави пов'язані із надмірною відкритістю і гласністю, нерозумінням і недооцінкою необхідності охорони таємниць держави, і якщо додати правовий нігілізм у цій сфері діяльності, то можна констатувати — все це створило передумови для витoku відомостей політичного, економічного, науково-технічного і навіть оборонного характеру. Україна опинилася в епіцентрі стратегічних інтересів транснаціональних фінансово-промислових груп і корпорацій, які з великою зацікавленістю до накопиченого в Україні інформаційно-інтелектуального потенціалу стимулювали вільний і необмежений обмін знаннями наших вчених і спеціалістів із світовим науковим товариством, виїзд їх на роботу і продовження досліджень за кордоном. У нашій країні широким фронтом розпочали діяти різні іноземні фонди і «благодійні» організації, які під гаслом

підтримки економічних реформ і вітчизняної науки здійснювали безконтрольне викачування інформаційних ресурсів, особливо пов'язаних з науковими дослідженнями і розробками. За оцінками фахівців колишнього Державного комітету України з питань державних секретів, на початку 1994 року на території України діяло 42 таких «благодійних» іноземних фонди й організації.

Характерною особливістю того періоду було те, що державні органи, підприємства, установи і організації та їхні посадові особи фактично не керувалися нормативними документами, такими як Перелік найголовніших відомостей, що становлять державну таємницю СРСР, та відповідними радянськими відомчими переліками, а правоохоронні органи не бралися давати правову оцінку правопорушенням у сфері охорони державної, службової і військової таємниць.

У квітні 1992 року Кабінет Міністрів України за поданням Служби безпеки України своїм протокольним рішенням «Про захист таємної і службової інформації» (від 13 квітня 1992 року, протокол № 5) звертає увагу керівників усіх рівнів про відповідальність за забезпечення режиму секретності, здійснення належних заходів для збереження державної, службової і військової таємниць, виключення випадків несанкціонованої передачі за межі України документів, матеріалів, виробів, технологій, що містять інформацію з обмеженим доступом.

За дорученням Кабінету Міністрів України Мінмашпромом, Мінпромом, МО, СБУ, Президією НДН України та іншими міністерствами і відомствами розробляється Тимчасовий перелік відомостей, опублікування яких обмежується, та Положення про порядок підготовки матеріалів, призначених для відкритого опублікування, які вводяться в дію постановою Кабінету Міністрів України від 21 липня 1992 року № 419. Дію Тимчасового переліку було встановлено до прийняття Закону України «Про державну таємницю».

Важливим кроком у формуванні системи захисту інформації стало прийняття Верховною Радою України Закону «Про інформацію» від 2 жовтня 1992 року, яким передбачено формування загальної системи охорони інформації і утворення відповідних органів спеціальної компетенції для здійснення державної інформаційної політики у цій сфері (ст. 6). Законом також була визна-

чена інформація, що підлягає охороні (ст. 30) і передбачена необхідність встановлення режиму доступу до неї (ст. 29).

Прийняття Закону України «Про інформацію» прискорило утворення державних органів спеціальної компетенції у сфері захисту інформації. Постановою Кабінету Міністрів України від 2 березня 1993 року № 156 утворюються Державна служба України з питань технічного захисту інформації, на яку покладаються функції реалізації державної політики, організаційного, нормативно-методичного забезпечення технічного захисту інформації (ДСТЗІ України). Постановою Уряду від 4 травня 1993 року № 327 утворюється Державний комітет України з питань державних секретів України (Держкомсекретів України). Функції комітету передбачали: забезпечення ним реалізації державної політики з питань державних секретів; реєстрацію відомостей, що становлять державну таємницю; організацію, координацію і контроль режимно-секретної діяльності державних органів, органів регіонального і місцевого самоврядування, підприємств, установ і організацій незалежно від форм власності, дипломатичних представництв та інших об'єктів України за кордоном.

Постановою Кабінету Міністрів України від 28 травня 1993 року № 377 утворюється Державний комітет України по охороні державних таємниць у пресі та інших засобах масової інформації як спеціально уповноважений орган державної виконавчої влади для здійснення державної інформаційної політики у цій сфері діяльності.

Протягом другої половини 1993 року спеціально уповноваженими державними органами у сфері захисту інформації формуються центральні органи та їх територіальні підрозділи, здійснюється активний пошук доцільних підходів до організації, координації діяльності щодо захисту інформації, форм і методів контролю за станом цієї роботи, розробляються вітчизняні нормативно-правові основи захисту інформації.

¹ Завершенням першого етапу формування і становлення системи захисту інформації доцільно вважати прийняття Верховною Радою України Закону України «Про державну таємницю». Вперше в історії України на рівні закону визначені: порядок встановлення обмежень до відомостей, що становлять державну таємницю; правові основи регулювання суспільних відносин у сфері охорони таємної інформації. А також створена відповід-

на правова база для розробки нормативно-правових, методичних та інших керівних документів у сфері захисту інформації.

Розглядаючи другий етап (січень 1994 — березень 1999 року), доцільно обмежитися наведеним строком з таких причин. Закон України «Про державну таємницю» визначає компетенцію державних органів у сфері реалізації державної політики щодо державної таємниці та спеціально уповноважені органи у сфері захисту інформації. Було встановлено, що спеціально уповноваженим центральним органом державної виконавчої влади у сфері забезпечення державної таємниці є Державний комітет України з питань державних секретів, а окремі функції у цій сфері щодо технічного захисту інформації, оперативних заходів охорони державної таємниці, фельд'єгерського зв'язку, охорони державної таємниці у засобах масової інформації виконують державні органи в межах повноважень, передбачених законодавством. Завершення цього етапу доцільно пов'язувати із ліквідацією Держкомсекретів України Указом Президента України від 13 березня 1999 року у зв'язку із черговим етапом адміністративної реформи.

Держкомсекретів України був головним організатором і розробником Закону України «Про державну таємницю», нормативно-правових, науково-методичних і організаційних основ, які дали змогу створити національну систему охорони державної таємниці та вдосконалювати інші напрями захисту інформації спільно із державними органами, визначеними для виконання окремих функцій у цій сфері діяльності.

Дуже важливо, що Закон України «Про державну таємницю» чітко визначив компетенцію державних органів у сфері нормативно-правового регулювання відносин, пов'язаних з охороною державної таємниці.

На виконання вимог Закону України «Про державну таємницю» та постанови Верховної Ради України «Про порядок введення в дію Закону України «Про державну таємницю» Держкомсекретів України спільно із державними органами, на які було покладено окремі функції у сфері охорони державної таємниці (ДСТЗІ України, Держкомтаємниць України, СБ України), всіма міністерствами і відомствами розпочали активну роботу по опрацюванню нормативно-правової бази. Уже у квітні 1994 року вводяться в дію перші нормативно-правові докумен-

ти з питань охорони державної таємниці. Указом Президента України від 23 квітня 1994 року затверджується Положення про державного експерта з питань таємниць, яким регламентується діяльність державних експертів щодо порядку і правил віднесення відомостей до державної таємниці, їх обов'язки, права, система взаємодії з державними органами, підприємствами, установами і організаціями та спеціально уповноваженим державним органом у сфері охорони державної таємниці. Постановою Кабінету Міністрів України від 29 квітня 1994 року затверджується Положення про порядок і механізм формування та опублікування Зводу відомостей, що становлять державну таємницю³⁵⁸.

Наступним важливим нормативно-правовим документом, введеним в дію у 1994 році, є Положення про порядок і умови надання органам державної виконавчої влади, підприємствам, установам і організаціям дозволу (ліцензії) на здійснення діяльності, пов'язаної з державною таємницею, та про особливий режим цієї діяльності (затверджене постановою Кабінету Міністрів України від 20 червня 1994 року). На виконання вимог Закону України «Про державну таємницю» цей нормативно-правовий документ, підготовлений з урахуванням досвіду розвинутих країн, передбачав провадження діяльності з використанням державної таємниці лише на підставі дозволу (ліцензії) Держкомсекретів України, і тільки після створення необхідних умов режимно-секретного забезпечення цього виду діяльності³⁵⁹.

У 1994 році державними органами, в тому числі спеціально уповноваженим державним органом у сфері охорони державної таємниці, вводяться в дію керівні, рекомендаційні і методичні документи з питань", забезпечення виконання чинного законодавства про державну таємницю та першочергових заходів щодо захисту державних секретів; удосконалення роботи режимно-секретних органів; здійснення розробки Зводу відомостей, що становлять державну таємницю України, та на їх основі відомих розгорнутих переліків такої інформації та ін.

Характерною особливістю 1994 року є те, що з урахуванням вимог чинного законодавства в нашій країні Верховною Радою приймається перший у сфері захисту інформації Закон України «Про захист інформації в автоматизованих системах» (від 5 липня 1994 року). Саме на виконання вимог закону та постанови Кабі-

нету Міністрів України від 9 вересня 1994 року №632 затверджується Положення про технічний захист інформації в Україні.

Кабінетом Міністрів України постановою від 13 січня 1995 року «Про заходи щодо виконання Постанови Верховної Ради України від 5 липня 1994 року «Про введення в дію Закону України «Про захист інформації в автоматизованих системах» та статті 34 Закону України «Про державну таємницю» на Державну службу України з питань технічного захисту інформації покладалося: здійснення управління захистом інформації в автоматизованих системах, координацію роботи вітчизняної служби захисту інформації з відповідними органами інших країн, а також видачу спеціальних дозволів (ліцензій) щодо технічного захисту інформації відповідно до ст. 20 Закону України «Про захист інформації в автоматизованих системах»³⁶⁰, а також була схвалена Програма робіт з організації, стандартизації та сертифікації в галузі технічного захисту інформації на 1995—1998 роки. Відповідно до цієї програми здійснювалася розробка нормативних та розпорядчих документів щодо: виготовлення та сертифікації засобів технічного захисту інформації від витоку інформації радіотехнічними, акустичними, оптичними та іншими каналами; розробляється перелік продукції, яка підлягає обов'язковій сертифікації в галузі технічного захисту інформації; формуються основи для створення органів сертифікації випробувальних лабораторій для засобів технічного захисту інформації та ліцензування діяльності з питань технічного захисту інформації.

У той час наказами ДСТЗІ України вводяться в дію: Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (9 червня 1995 року № 25); Тимчасове положення про категоріювання об'єктів (10 липня 1995 року № 35).

Доцільно нагадати і про те, що переломом для формування національної системи захисту інформації стає 1995 рік з погляду застосування нових підходів до охорони державної таємниці та певною мірою технічного захисту інформації. У цей рік вперше в історії України з'являються власні документи, що визначають відповідно до чинного законодавства інформацію, віднесену до державної таємниці. Наказом Держкомсекретів України

від 31 липня 1995 року №47 зареєстровано у Мін'юсті України і вводиться в дію Звід відомостей, що становлять державну таємницю України, та розроблені на його основі, погоджені із Держкомсекретів України і затверджені державними експертами з питань таємниць відомчі переліки відомостей, віднесених до державної таємниці³⁶¹. Кабінетом Міністрів України затверджується Положення про режимно-секретні органи в міністерствах, відомствах, уряді Автономної Республіки Крим, місцевих органах державної виконавчої влади, виконкомах Рад, на підприємствах, установах і організаціях (постанова від 4 серпня 1995 року № 609), тобто нормативним документом відповідно до нових політичних і соціально-економічних умов регламентується порядок утворення, реорганізації і ліквідації та діяльність режимно-секретних органів, їх статус і роль у системі управління державними органами, підприємствами, установами і організаціями з погляду охорони державної таємниці³⁶².

21 грудня 1995 року в Кабінеті Міністрів України була проведена нарада з питання про хід виконання Закону України «Про державну таємницю» та актуальні завдання органів державної виконавчої влади у сфері захисту державної таємниці. У нараді взяли участь керівники міністерств, відомств та інших центральних установ України, Автономної Республіки Крим, обласних, Київської та Севастопольської міських державних адміністрацій, на яких покладено функціональні обов'язки організації та координації робіт по захисту державної таємниці, відповідальні працівники Держкомсекретів України. У рішенні наради відзначено, що в 1993—1995 роках в Україні здійснено комплекс організаційно-правових і практичних заходів, що стало передумовою створення і функціонування власної системи захисту державної таємниці. Нарада визначила комплекс актуальних завдань органів державної виконавчої влади з питань удосконалення діяльності по забезпеченню виконання чинного законодавства про державну таємницю.

У 1996 році в Україні відбулися важливі події, які безпосередньо впливали не тільки на подальший розвиток державності, а й на систему захисту інформації та управління цією системою з боку держави.

28 червня 1996 року Верховна Рада прийняла Конституцію України. Утворення, реорганізація та ліквідація міністерств та

інших центральних органів за поданням Прем'єр-міністра України Основним Законом України було віднесено до повноважень Президента України (ст. 106).

Указом Президента України від 26 липня 1996 року «Про зміни в системі центральних органів виконавчої влади України» були ліквідовані Державний комітет України з питань державних секретів і Державна служба України з питань технічного захисту інформації, а на їх базі утворений Державний комітет України з питань державних секретів та технічного захисту інформації, на який покладається координація режимно-секретної роботи та функціонування інфраструктури системи технічного захисту інформації центральних та місцевих органів виконавчої влади, підприємств, установ і організацій усіх форм власності, дипломатичних представництв та інших об'єктів України за кордоном.

Зосередження в одному державному органі функцій щодо забезпечення реалізації державної політики у сфері охорони державної таємниці та технічного захисту інформації, а також затвердження Указом Президента України нормативних документів, що регламентують цю діяльність, сприяли підвищенню ефективності роботи і можливостей нового органу державної виконавчої влади у сфері захисту інформації. Водночас слід зауважити, що виконання ліквідаційних заходів та формування структурних підрозділів, нового комітету в центрі і в регіонах відвертало значні сили від виконання функцій, пов'язаних із забезпеченням функціонування системи охорони державної таємниці та технічного захисту інформації.

У складних умовах продовження економічних та адміністративної реформ, розширення міжнародних зв'язків України, Державний комітет України з питань державних секретів та технічного захисту інформації в цілому забезпечив формування та проведення збалансованої державної політики в сфері охорони державної таємниці, функціонування інфраструктури технічного захисту інформації, організацію, координацію і контроль за станом режимно-секретної роботи. Тривала активна робота щодо подальшого удосконалення інформативно-правового забезпечення охорони державної таємниці та технічного захисту інформації.

Постановою Кабінету Міністрів України від 30 липня 1996 року затверджується Положення про порядок надання, скасування та переоформлення допуску громадян України до державної таємниці. Цей нормативний документ чітко регламентував порядок і правила діяльності керівників державних органів, підприємств, установ і організацій та їх режимно-секретних органів, строки проведення підрозділами СБ України спеціальних перевірок, пов'язаних з допуском до державної таємниці і порядок реалізації результатів перевірок та права і обов'язки громадян, стосовно яких вирішувалися питання стосовно допуску до державної таємниці³⁶³.

Розробляються і вводяться в дію Інструкція про порядок відбору та передачі секретних документів на архівне зберігання (затверджено наказом Держкомсекретів та Головархіву України від 3 березня 1997 року № 25/7)³⁶⁴, Типове положення про секретний архівний підрозділ державного органу, підприємства, установи і організації (затверджено наказом Держкомсекретів і Головархіву України від 3 березня 1997 року № 26/8)³⁶⁵.

Відповідно до ст. 33 Закону України «Про державну таємницю» спільно із зацікавленими державними органами розробляються і вводяться в дію нормативно-правові акти, що регулюють особливості здійснення наглядових, контрольно-ревізійних та інших функцій органів державної влади щодо підприємств, установ і організацій, діяльність яких пов'язана з державною таємницею (органів прокуратури, державних податкових інспекцій, держкомнаглядохоронпраці, контрольно-ревізійною службою, аудиторськими підрозділами Спілки аудиторів тощо)³⁶⁶.

На виконання ст. 31 Закону України «Про державну таємницю» розробляються і рішеннями Президента України та Кабінету Міністрів України вводяться в дію ряд нормативних документів про порядок оформлення дозволів за розпорядженнями Президента України щодо передавання іншій державі інформації, що становить державну таємницю, та носіїв такої інформації, укладання міжнародних договорів щодо охорони державних секретів; проведення експертиз у галузі експертного контролю; охорони державної таємниці, а також іншої інформації з обмеженим доступом, що є власністю держави в процесі роботи з іноземцями та ін. Введення в дію наведених нормативних документів сприяло подальшому розвитку міжнародного

співробітництва з використанням інформації, віднесеної до державної таємниці, та в межах правового поля держави забезпечувати захист національних інтересів, пов'язаних з державними секретами.

Актуальною проблемою для України залишалося розсекречування матеріальних носіїв секретної інформації колишнього СРСР. Україна в спадщину від СРСР отримала близько 133 млн. таємних документів та понад 50 тис. виробів з грифами секретності. Враховуючи, що протягом року державними експертами з питань таємниць щорічно проводилося близько 500 експертиз таких матеріалів, для розсекречування накопичених носіїв секретної інформації колишнього СРСР потрібно було б майже 25 років. Сьогодні очевидно, що спроба вирішити ці питання зусиллями державних експертів з питань таємниць було помилкою Держкомсекретів України. Необхідна була вітчизняна нормативна основа з урахуванням досвіду Росії, в якій розсекречування носіїв секретної інформації колишнього СРСР здійснювалася на підставі нормативного документа, затвердженого урядом Російської Федерації.

Державний комітет з питань державних секретів та технічного захисту інформації здійснював активні заходи щодо вдосконалення правових і організаційних основ охорони державної таємниці та технічного захисту інформації. Так, протягом 1997 — 1998 років здійснюється розробка проектів Законів України «Про внесення змін і доповнень до Закону України «Про державну таємницю» та «Про внесення змін і доповнень до Кодексу України про адміністративні правопорушення щодо встановлення відповідальності за порушення законодавства про державну таємницю». Ці проекти законів були погоджені в заінтересованих міністерствах, відомствах і пройшли експертизу у другому півріччі 1998 року в Кабінеті Міністрів України, Раді національної безпеки і оборони України та Адміністрації Президента України.

Особлива увага приділялася Державним комітетом з питань державних секретів та технічного захисту інформації України розвитку проекту Інструкції про порядок забезпечення режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях України, яка призначена стати основним нормативним доку-

ментом і охопити всі аспекти організації робіт з забезпечення режиму секретності в Україні та повною мірою замінити нормативний документ колишнього СРСР, відомий спеціалістам як Інструкція 0126-87 р. Проект інструкції, погоджений із заінтересованими державними органами, на початку 1999 року комітетом був внесений на розгляд Кабінету Міністрів України.

Постановою Кабінету Міністрів України від 8 жовтня 1997 року №1126 була затверджена Концепція технічного захисту інформації в Україні, яка визначила основи державної політики у сфері захисту інформації інженерно-технічними заходами та передбачила забезпечення єдності принципів формування і проведення такої політики в усіх сферах життєдіяльності особи, суспільства, держави та слугувала основою для розвитку системи технічного захисту інформації³⁶⁷. Розробляються і наказом Держкомсекретів України (від 22 травня 1997 року № 51) вводяться в дію: Рекомендований перелік нормативно-правових актів та нормативних документів з питань технічного захисту інформації, Рекомендований перелік нормативно-технічних документів для використання при проведенні ліцензованих видів робіт у галузі технічного захисту інформації.

Спільно із Держстандартом України розробляються і вводяться в дію ряд державних стандартів сфери технічного захисту інформації, серед яких:

- ДСТУ 3396 0-96. Захист інформації. Технічний захист інформації. Основні положення",

- ДСТУ 3396 1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт;

- ДСТУ 1. 3-93. Порядок розроблення, побудови, викладу, оформлення, узгодження, затвердження, позначення та реєстрації технічних умов;

- КНД 50-009-93. Типова побудова технічних умов³⁶⁸.

Державним комітетом організовується з 1996 року система перепідготовки та закладаються основи для підготовки кадрів для системи підготовки системи таємниці та технічного захисту інформації. На базі НТУ України Київського політехнічного інституту створюються і функціонують спеціальні курси післядипломної освіти «Організація захисту секретної інформації», на базі КМУЦА спеціальні курси «Автоматизація обробки секретної інформації». За поданням Держкомсекретів і Міносвіти

Кабінетом Міністрів України були відкриті нові напрями підготовки фахівців за спеціальностями: захист інформації з обмеженим доступом та автоматизація її обробки; система захисту від несанкціонованого доступу; адміністративний менеджмент у сфері захисту інформації; захист інформації в комп'ютерних системах та мережах.

У цей період здійснено комплекс заходів для удосконалення організації, координації та контролю за станом режимно-секретної роботи та технічного захисту інформації, а також для надання методичної допомоги режимно-секретним органам і підрозділам технічного захисту інформації. Аналізувався позитивний досвід практичної діяльності територіальних підрозділів Державного комітету України з питань державних секретів та технічного захисту інформації.

Керівництво Держкомсекретів України усвідомлювало, що формування і забезпечення системи захисту інформації здійснюється в умовах політичних і соціально-економічних змін, подальшого розвитку міждержавного співробітництва, при яких раніше налагоджені механізми захисту інформаційних ресурсів не повною мірою відповідають новим умовам і в деяких випадках втрачають свою ефективність. За ініціативою комітету, підтриманою на всіх рівнях державної влади, протягом 1997 року була розроблена Державна програма розвитку системи охорони державної таємниці та технічного захисту інформації в Україні на 1999—2003 роки. Її після узгодження із заінтересованими міністерствами і відомствами на початку 1998 року було подано на розгляд Кабінету Міністрів України та надіслано до Мінекономіки і Мінфіну для врахування при підготовці проекту на 1999 рік.

Однак у результаті перерозподілу функцій щодо охорони державної таємниці та технічного захисту інформації, тобто на дві системи, коштів на Державну програму розвитку системи охорони державної таємниці та технічного захисту інформації на 1999—2003 роки, на подальший розвиток нормативно-правового, науково-методичного та інженерно-технічного забезпечення охорони державної таємниці та технічний захист інформації на 1999 рік не передбачалося.

Найбільш складною була ситуація щодо організаційного забезпечення і правового регулювання відносин, пов'язаних із

захистом інформації із обмеженим доступом, що не становить державної таємниці. Нагадаємо, що 1993 році був утворений Державний комітет України з охорони державних таємниць у засобах масової інформації. У процесі реформування державних органів і утворення нових (Мінпресінформ, Мінінформ, Держкомінформ) функції щодо організації, координації і контролю захисту інформації з обмеженим доступом, що не становить державної таємниці, втрачені. Фактично реальністю стало те, що в Україні відповідними органами законодавства та розробленими на їх основі нормативними документами регулюються суспільні інформаційні відносини лише пов'язані з державною і банківською таємницями. Стосовно інших передбачених законодавством таємниць та конфіденційної інформації (близько трьох десятків видів) чинні закони не передбачають правових механізмів захисту. Без визначення на рівні закону (законів) правового режиму кожного виду інформації з обмеженим доступом, що не становить державної таємниці, не можна без збитків для людини, суспільства і держави встановити цивілізовані інформаційні відносини як усередині країни, так і в процесі міжнародного інформаційного співробітництва.

На основі аналізу стану та перспектив розвитку національного законодавства сфери захисту інформації, проведеного Держкомсекретів України, було розроблено проект Закону України «Про інформацію з обмеженим доступом, що не становить державної таємниці», позитивно сприйнятий науковою громадськістю, науковими спеціалістами, він отримав і позитивний відгук Інституту законодавства Верховної Ради України.

Водночас Держкомсекретів, Головархів і СБ України здійснили спільну розробку проекту Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави. Розробка законопроекту та інструкції, спрямованої на виконання його правових норм, була обумовлена ст. 34 Конституції України та стандартами Європейського Союзу про те, що обмеження прав на інформацію у демократичному суспільстві може бути введено тільки законом. Наприкінці 1998 року постановою Кабінету Міністрів України ця інструкція була затверджена і набула чинності. Отже, обме-

ження прав на таку інформацію до цього часу регламентується на рівні подзаконного акта, а це вимагає невідкладних заходів щодо прийняття відповідного закону для регулювання суспільних інформаційних відносин стосовно правового режиму інформації з обмеженим доступом, що не становить державної таємниці.

На початку 1998 року в межах чергового етапу адміністративної реформи функції щодо забезпечення реалізації державної політики в галузі захисту державних інформаційних ресурсів у мережах передачі даних та технічного захисту інформації передаються Службі безпеки України, а Указом Президента України від 10 квітня 2000 року у СБУ утворюється Департамент спеціальних телекомунікаційних систем та захисту інформації як орган державного управління.

Проведенням ліквідаційних заходів протягом березня—липня 1999 року, переданням відповідному підрозділу Служби безпеки України функцій та матеріально-технічних ресурсів завершилася діяльність Державного комітету України з питань державних секретів, який протягом шести років розробляв пропозиції щодо державної політики у сфері охорони державної таємниці та безпосередньо здійснював її реалізацію. Протягом дворічного виконання функцій у сфері технічного захисту інформації, вжитими заходами була впорядкована система правового і організаційного забезпечення цього напрямку діяльності та закладено основи для його подальшого розвитку. Творчий наробок працівників Держкомсекретів України є вагомим свідченням актуальності і необхідності створення системи організаційного і правового забезпечення захисту інформації з обмеженим доступом.

Служба безпеки України, починаючи з середини 1999 року, крім спеціальних функцій, у повному обсязі забезпечує реалізацію державної політики у сфері охорони державної таємниці (організаційне, нормативно-правове забезпечення, координація цієї діяльності та контроль за її станом). Нагадаємо, що у 1998 році на відповідний підрозділ СБУ України покладені функції реалізації державної політики в галузі захисту державних інформаційних ресурсів у мережах передачі даних, криптографічного та технічного захисту інформації, а з квітня 2000 року Департамент спеціальних телекомунікаційних систем та захисту

інформації СБ України (ДСТСЗІ) визначено як орган державного управління. Надання ДСТСЗІ СБ України такого статусу пояснюється тим, що ряд його функцій, визначених нормативними документами, мають загальнодержавне значення, а рішення департаменту, прийняті у межах його компетенції, мають обов'язковий характер для всіх суб'єктів України.

Зусиллями СБ України було прискорено прийняття Закону України «Про державну таємницю» в редакції від 21 вересня 1999 року і введення в дію Закон України «Про внесення змін до Кодексу України про адміністративні правопорушення щодо встановлення відповідальності за порушення законодавства про державну таємницю» від 21 вересня 1999 року.

Досвід роботи у сфері захисту інформації та проведення протягом 1999 — 2003 років досліджень дають змогу зробити висновки про те, що система захисту інформації важко справляється із постійним зростанням джерел загроз і небезпек, не оцінює достатньо стан безпеки в інформаційній сфері і не блокує загроз. Тому існуючі концептуальні підходи до захисту інформації, які впливають із парадигми — безпека інформації та сфери її обігу є захист від загроз і небезпек, потребує корекції. Пропонується змінити парадигму і розглядати захист інформації не як захист від загроз і небезпек, а як об'єкта управління, тобто в основу вирішення цих питань покласти функціональний підхід.

З визначення головної мети і функцій впливатиме логічна модель державного управління національними інформаційними ресурсами та їх захистом, а саме: головна мета — функції — структура. На підставі головної мети розробляються основні функції (а не навпаки), які дають змогу сформувати ієрархічну структуру центральних, регіональних і місцевих органів виконавчої влади. У випадку, коли змінюється головна мета, мають бути розроблені додаткові або нові функції та внесені зміни до структури державних органів, що задовольнятиме досягнення нової головної мети. Відповідно до головної (стратегічної) мети розробляються і впроваджуються системні заходи правового та організаційного забезпечення, спрямовані на її здійснення. Функціональний підхід до формування системи захисту інформаційних ресурсів виключатиме можливість втрати будь-яких функцій у процесі формування державних органів.

Потребує вдосконалення сама організаційна структура державного управління системного захисту інформації, оскільки Україною було обрано не найкращий варіант створення загальної системи захисту інформації. Під кожний напрям діяльності утворювався автономний і самостійний орган управління, який виконував свої завдання фактично ізольовано від загальної стратегічної мети, спрямованої на забезпечення національної безпеки (державна таємниця, технічний захист інформації, засоби масової інформації та інформація з обмеженим доступом тощо). Зростання кількості державних структур значно збільшує затрати держави на управлінську діяльність, розпорошує її і веде до неефективного використання фінансових ресурсів.

Реальністю є те, що в державі створена громіздка і розпорошена структура державних органів. Не вирішує проблеми і зосередження функцій щодо державної таємниці та технічного захисту інформації в одному державному органі. Захист інформації та сфери її обігу має міжвідомчий характер, стосується діяльності всіх державних органів. Відсутність ефективно діючих правових і організаційних механізмів регулювання взаємодії під час розробки і реалізації загальнодержавних рішень у сфері захисту інформації породжує міжвідомчі комісії. І головне — міжвідомча конкуренція і суперечності не дають змоги в повному обсязі реалізувати можливості у сфері захисту інформації, які є в державі: економічні, матеріально-технічні, інтелектуальні, інформаційні тощо. Так, міжвідомчі колізії фактично поховали Державну програму розвитку системи охорони державної таємниці та технічного захисту інформації на 1999 — 2003 роки. Подальший розвиток системи захисту інформації в Україні здійснювався лише на напрямках державних секретів та технічного захисту інформації. Стосовно інформації з обмеженим доступом, що не становить державної таємниці, проблемні питання щодо правового і організаційного забезпечення залишаються не вирішеними й досі.

Міжвідомчі колізії вкрай негативно впливають на правотворчий процес, який щодо сфери захисту інформації здійснюється шляхом розв'язання окремих проблем в окремих законах та підзаконних актах фрагментарно. У цьому процесі беруть участь різні державні органи та наукові школи, які здебільшого прагнуть обстоювати власні інтереси.

Деякі приклади. Верховною Радою України 5 липня 1994 року був прийнятий Закон України «Про захист інформації в автоматизованих системах». Серед його розробників і народних обранців отримали перевагу погляди на систему технічного захисту інформації як прерогативу не держави, а установ і організацій. У законі стосовно служб захисту інформації була визначена така правова норма: «У державних установах та організаціях можуть створюватись підрозділи, служби, які організовують роботу, пов'язану із захистом інформації, підтримки рівня захисту інформації в АСУ» (ст. 15). В умовах складного економічного стану, остаточного принципу фінансування робіт щодо охорони державної таємниці та технічного захисту інформації, який склався на той час, керівники державних органів підприємств, установ і організацій, керуючись правовою нормою, що вони «можуть створювати» вказані підрозділи і служби, упродовж 1994 року закінчили ліквідацію, а в деяких випадках скорочення до окремих осіб органів, які раніше мали назву підрозділів протидії іноземним технічним розвідкам. Сьогодні можна зробити висновок про те, що подальша недооцінка необхідності технічного захисту інформації та передумови майбутнього так званого касетного скандалу були закладені ще в 1994 році.

Із наведеним прикладом тісно пов'язаний і наступний. Супроводження Національної програми інформатизації, передбаченої Законом «Про національну програму інформатизації» від 4 лютого 1998 року, було покладено на Державний комітет України зв'язку та інформатизації. Вузьке відомче ставлення до розвитку Національної програми інформатизації, інших програм і проектів інформатизації призвело до ігнорування вимог чинного законодавства про віднесення витрат на впровадження заходів і засобів захисту інформації до собівартості робіт. Інформаційно-телекомунікаційні системи створювалися за архітектурою відкритих систем. Для усунення негативних наслідків для захисту інформації в таких системах потрібен тривалий час.

В Україні періодично вживаються заходи для забезпечення координації на державному рівні діяльності щодо державної інформаційної політики та інформаційної безпеки та її складової безпеки інформаційних ресурсів і сфери їх обігу. Указом Президента України від 3 лютого 1998 року при Раді національ-

ної безпеки і оборони України була створена Комісія з питань інформаційної безпеки. Майже через два роки ця комісія була ліквідована. На підставі рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки» Указом Президента України утворена Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки з функціями координації і контролю діяльності щодо виконання заходів формування і захисту національного інформаційного простору, забезпечення безпеки у цій сфері, розробки і підготовки проектів відповідних нормативно-правових документів³⁶⁹. Супроводження діяльності Міжвідомчої комісії покладено на апарат РНБО України. Незважаючи на високий рівень фахової підготовки апарату РНБО України, забезпечити у повному обсязі виконання функцій, покладених на Міжвідомчу комісію, він не зможе. Для цього потрібно значно збільшити апарат РНБО України за рахунок спеціалістів з питань інформаційної політики, інформаційної безпеки та захисту інформації.

Окрім того, Міжвідомча комісія з питань інформаційної безпеки не зможе взяти на себе функції органів виконавчої влади, компенсувати своєю діяльністю ті ланки, що виконують функції не в повному обсязі, а також функції, які в організаційному і правовому планах залишилися не визначеними.

Один із варіантів розв'язання означених проблем полягає в зміцненні організаційного, кадрового і матеріального забезпечення спеціально уповноважених органів державної влади, що здійснюють управління конкретними напрямками інформаційної діяльності та інформаційної безпеки. А також на основі функціонального підходу чітко визначити компетенцію державних органів усіх рівнів та їхню відповідальність за станом інформаційної безпеки та безпеки інформації у сфері її обігу.

Найбільш прийнятним варіантом може бути з огляду на те, що керівництво у сфері національної безпеки Конституцією України покладено на Президента України, його рішенням перетворити Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки на орган державного управління, підпорядкований безпосередньо главі держави. За рахунок кадрових, матеріально-технічних і фінансових ресурсів розпоро-

шених державних органів, що виконують окремі функції у сфері захисту інформації, сформувати апарат Міжвідомчої комісії.

Колегіальне керівництво державним органом, що здійснює державну політику такої складної багатопланової сфери, як інформаційна політика та інформаційна безпека виключатиме міжвідомчі колізії, що сприятиме ефективнішому захисту національних інтересів у цій найбільш чутливій сфері національної безпеки. А державне управління із єдиного центру забезпечуватиме ефективнішу координацію правотворчого процесу, діяльності державних органів, науково-методичного забезпечення, виключить можливість розпорошення державних коштів на вирішення цих питань.

Окрім того, слід урахувати, що необхідність такого підходу впливатиме із курсу України на побудову правової демократичної держави, розвитку громадянського суспільства, необхідності встановлення цивільного контролю над Збройними Силами та іншими силовими структурами. Система захисту інформації та сфери її обігу як комплекс заходів з боку держави з цивілізованого обмеження певних прав і свобод громадян та суспільних організацій — важливий показник розвитку демократії в будь-якій країні.

4.2. ПРОБЛЕМИ ЩОДО СТВОРЕННЯ ПРАВОВИХ ПЕРЕДУМОВ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Правові відносини в інформаційній сфері, в тому числі захист інформаційних ресурсів, регулюються національною системою законів і підзаконних актів.

Результати аналізу правових норм інформаційного законодавства, а саме: правових інформаційних норм, що містить Конституція України; правових норм, які безпосередньо стосуються інформації як об'єкта правовідносин та її захисту, а також процесу інформатизації; правових норм, які регулюють окремі суспільні відносини в інформаційній сфері стосовно права власності на інформацію та міжнародних договорів, угод, які укладені Україною або до яких приєдналася наша держава, свідчать про те, що інформаційне законодавство не є адекватним реаліям суспільства і неспроможне ефективно забезпечити

правовий захист як права громадян на інформацію, так і власне інформацію, яка підлягає охороні відповідно до чинних нормативно-правових актів.

4.2.1. Проблеми у сфері захисту інформаційних ресурсів, віднесених до державної таємниці

Завдяки здійсненню у 1993 — 1995 роках в Україні комплексу організаційно-правових і практичних заходів, що стало передумовою створення і функціонування власної системи захисту державної таємниці, вжиття реальних кроків для її становлення у 1995 — 1999 роках можна стверджувати, що на даний час найбільш врегульованою сферою правових інформаційних відносин у суспільстві й державі є сфера, пов'язана з охороною державної таємниці.

Чинне законодавство про державну таємницю містить комплекс правових норм, що такий інститут права, як правовий режим інформації, віднесеної до державної таємниці, а також ряд правових норм, що регулюють відносини, пов'язані з дозвільним порядком провадження діяльності щодо створення і використання відомостей, що містять державну таємницю як у середині країни, так і в процесі співробітництва з іноземними партнерами. При цьому доречно нагадати, що національна система охорони державної таємниці розроблялася з урахуванням досвіду США³⁷⁰, Російської Федерації³⁷¹, Франції³⁷², Німеччини³⁷³, КНР³⁷⁴ та інших країн (*Оцінка чинної правової бази України у сфері охорони державної таємниці надана у п. 4.1*).

Характеризуючи національну систему правового регулювання відносин у сфері охорони державної таємниці, слід підкреслити, що *нормативно-правове забезпечення і в цій, найбільш врегульованій сфері, ще недосконале, не враховує важливих аспектів процесів і змін, які відбуваються в суспільстві, особливостей соціального, державного устрою та деяких аспектів охорони державної таємниці, що є у світовій практиці*.

Розглянемо найважливіші проблеми нормативно-правового регулювання правових відносин, пов'язаних з охороною інформаційних ресурсів, віднесених до державної таємниці.

Визначальною проблемою для сфери діяльності, пов'язаної з державною таємницею, є відсутність наукового політичного і

соціально-економічного обґрунтування критеріїв і методик віднесення інформації до державної таємниці.

Закон України «Про державну таємницю»³⁷⁵ містить правові норми, які визначають інформацію у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, що може бути віднесена до державної таємниці. Правові норми цього закону вимагають від державних експертів з питань таємниць визначати підстави для віднесення інформації до державної таємниці, обґрунтовувати шкоду, завдану національній безпеці України у разі її розголошення, та ступінь секретності зазначеної інформації. Ступінь секретності, відповідно до цього закону, — «категорія, яка характеризує важливість секретної інформації, ступінь доступу до неї та рівень її охорони з боку держави».

Таким чином, віднесення інформації до державної таємниці має не тільки політичні, соціальні аспекти, а насамперед економічні, пов'язані з фінансовими витратами на охорону цієї інформації з боку держави та можливими втратами вигод від відкритого використання цієї інформації.

На початковому етапі формування системи охорони державної таємниці колишнім Держкомсекретів України було розроблено і введено в дію «Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення інформації до державної таємниці та ступеня їх секретності»³⁷⁶. Запропонований у цих рекомендаціях метод експертних оцінок дає змогу в однакових приблизних умовних одиницях визначати величину економічної шкоди та тяжкості інших негативних наслідків, що можуть бути спричинені життєво важливим інтересам України внаслідок розголошення або втрати відомостей, які віднесені чи мають бути віднесені до державної таємниці, та надання цим відомостям невідповідного ступеня секретності. Інших керівних або методичних документів щодо визначення підстав для віднесення інформації до державної таємниці в Україні немає.

В умовах початкового етапу формування національної системи охорони державної таємниці (1993—1994 роки), коли гостро постала проблема термінової розробки і введення в дію Зводу відомостей, що становлять державну таємницю України (ЗВДТ), запропонована методика свою роль виконала. Підстави для

віднесення інформації до державної таємниці державними експертами формулювалися відповідно до вищевказаних «Методичних рекомендацій». ЗВДТ був розроблений і в установленому законодавством порядку набув чинності. У системі охорони державної таємниці ЗВДТ є основним документом. Він визначає перелік інформації, яка підлягає охороні, важливість цієї інформації, ступінь обмеження доступу до неї та рівень захисту державою. До введення в дію ЗВДТ у державі склалося вкрай ненормальне становище з охороною державних секретів. Підприємства, установи, організації та їхні посадові особи нормативними документами колишнього СРСР, такими як Перелік найголовніших відомостей, що становлять державну таємницю СРСР, відповідними радянськими відомчими переліками фактично не керувалися. Правоохоронні органи давати правову оцінку порушенням у сфері охорони державної таємниці на підставі вищевказаних нормативних актів колишнього СРСР не вважали можливим. Усе це зумовлювало необхідність термінової розробки переліку відомостей, що становлять державну таємницю, і введення в установленому законодавством порядку ЗВДТ.

На початковому етапі розвитку нашого суспільства, коли Україна робила перші кроки як незалежна держава, визначення підстав для віднесення інформації до державної таємниці, керуючись вищезазначеним методом експертних оцінок «приблизного в умовних одиницях» для визначення шкоди, в тому числі економічної, що може бути спричинена інтересам держави, можна вважати виправданим. На той час держава володіла монопольним правом власності на інформаційні ресурси, що містять відомості, віднесені до державної таємниці, та іншу інформацію з обмеженим доступом. Указані інформаційні ресурси були створені за рахунок коштів державного бюджету, правом володіти, користуватися та розпоряджатися ними були уповноважені державні органи директивного управління.

Сучасний розвиток держави, перехід до ринкової економіки, розвиток міжнародних відносин створюють нові правовідносини в інформаційній сфері. Інформаційні ресурси стають об'єктом товарних відносин. У таких умовах метод «приблизного визначення в умовних одиницях» підстав для віднесення інформації до державної таємниці може призвести до негативних

наслідків, завдавати реальної шкоди життєво важливим інтересам держави та її національній безпеці.

Сьогодні в Україні потрібна методика визначення підстав для віднесення інформації до державної таємниці та для оцінки вартості шкоди в разі втрати або розголошення цієї інформації з урахуванням передусім економічних показників на державному рівні не розроблялася. Потрібна також і методика оцінки вартості інформації як товару взагалі та інформаційних послуг. Відсутність зазначених методик створює передумови для довільного й суб'єктивного визначення вартості завданої шкоди у разі порушень в інформаційній сфері, пов'язаних з державною таємницею (Детальний розгляд методики і практики віднесення інформації до категорії з обмеженим доступом та пропозицій щодо порядку визначення критеріїв цієї роботи див. у п. 2.3.3).

Показовим прикладом тут можуть слугувати події, пов'язані з Інститутом біології південних морів (Севастополь). Як повідомлялося в газеті «Сегодня» (19 вересня 1999 року), СБУ була відвернута спроба передання іноземній державі результатів досліджень біології південних морів, проведених двома інститутами за 35 років. Ці наукові матеріали не підлягають розсекречуванню і сьогодні, є національним надбанням і, як свідчить автор статті, «оцінюються в 200 млн. доларів США, а за іншими розрахунками, — в мільярди». А це означає, що в разі несанкціонованого передання за кордон (втрата для держави) вказаних наукових матеріалів, що містять інформацію, віднесену до державної таємниці, шкода державі буде завдана у розмірі 200 млн. дол. США або кількох мільярдів.

У зв'язку з вищенаведеним виникає питання про правові санкції, які слід було застосувати до винних, а саме: виходячи із завданої державі шкоди у розмірі 200 млн. доларів чи кількох мільярдів?

Наукове політичне і соціально-економічне обґрунтування підстав для віднесення інформації до державної таємниці сприятиме реальному запобіганню шкоди державі та раціональному використанню витрат і коштів на захист тільки тих відомостей, виток яких, втрата або несанкціоноване поширення може справді заподіяти шкоду національній безпеці держави. Безумовно, основою концептуальних засад захисту інформації, що становить державну таємницю, на думку фахівців, має бути

економічна доцільність, як це також обгрунтовано у дослідженнях³⁷⁷.

Важливою проблемою для держави залишається розсекречування та зниження грифів секретності матеріальних носіїв інформації, яким грифи секретності надавалися відповідно до правил та порядку, встановлених у колишньому СРСР.

Нагадаємо, що на підприємствах, в установах і організаціях накопичено великий масив секретних документів (за даними колишнього Держкомсекретів, — понад 130 млн.) та багато тисяч спецвиробів, яким було надано грифи секретності на підставі Переліку найголовніших відомостей, що становлять державну таємницю СРСР (затвердженого постановою Ради Міністрів СРСР 3 грудня 1980 року) та переліків відомостей, що є державною таємницею, міністерств та відомств колишнього СРСР. Зберігання та використання цих масивів носіїв секретної інформації здійснюється відповідно до режимно-секретних вимог, встановлених чинним законодавством України. При цьому не враховується, що в колишньому СРСР носії інформації з грифом «таємно» не належали до державної таємниці: вони мали категорію службової або військової таємниці. Згідно з чинним законодавством України інформація зі ступенем секретності «таємно» є державною таємницею. *Вказана правова норма автоматично класифікувала службову й військову таємницю колишнього СРСР як державну таємницю України.*

Ще одним важливим аспектом цієї проблеми є те, що на забезпечення режиму секретності під час зберігання і використання вказаних масивів грифованих матеріальних носіїв відволікаються значні кошти, стримується використання технологій подвійного призначення та наукових досягнень для розвитку народного господарства України. При цьому слід підкреслити, що зазначені матеріальні носії секретної інформації були створені за рахунок бюджетних коштів і є власністю держави.

Проведена міністерствами і відомствами інвентаризація виконуваних і незавершених НДДКР, незатребуваних спецвиробів і науково-технічної документації, які розроблялися та виготовлялися на замовлення силових структур колишнього СРСР і є носіями секретної інформації, не привела до логічного вирішення питання про їх подальше використання на користь державі. Головною причиною цього є те, що в Україні немає нор-

мативно-правових актів щодо порядку розсекречування або зниження грифів секретності документів і виробів, які були засекречені відповідно до нормативних вимог колишнього СРСР.

Не визначає правових норм для розв'язання цих питань і нова редакція Закону України «Про державну таємницю»³⁷⁸. Цей закон лише передбачає порядок дії керівників органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, де здійснювалося засекречування матеріальних носіїв інформації, правонаступників перелічених керівників та керівників вищого рівня, які після закінчення встановлених строків засекречування матеріальних носіїв інформації та у разі зниження визначеного державним експертом з питань таємниць ступеня секретності такої інформації, зобов'язані протягом 6 місяців забезпечити зміну грифа секретності або розсекречування цих матеріальних носіїв секретної інформації.

Правові норми, визначені вказаним законом щодо порядку розсекречування матеріальних носіїв секретної інформації України, не можуть бути застосовані для розсекречування інформаційних ресурсів, які залишилися від колишньої держави, у зв'язку з тим, що не враховують важливих аспектів цієї роботи, а саме:

— деякі з носіїв секретної інформації колишнього СРСР підпадають під категорію міждержавних секретів, як це визначено, укладеною у м. Мінську 22 січня 1993 року Угодою про взаємне забезпечення збереженості міждержавних секретів, підписаною й Україною³⁷⁹;

— у процесі розсекречування вказаних носіїв секретної інформації поряд з визначенням можливості їх відкритого використання або продовження строків дії відповідних грифів секретності має бути визначена на основі науково обгрунтованих критеріїв їхня наукова, культурна, історична цінність та доцільність віднесення до національного надбання;

— необхідність розробки і введення в дію нормативно-правових норм, які визначали б порядок участі державних експертів з питань таємниць у розсекречуванні, зниженні грифів секретності або продовженні строків дії цих грифів секретності, встановлених на матеріальних носіях секретної інформації колишнього СРСР.

Розсекречування міждержавних секретів, як цього вимагають правові норми, визначені мінською угодою від 22 січня 1993 року, може бути здійснене лише за погодженням з державами, які підписали її. Вирішення цього питання гальмується відсутністю механізму застосування цієї правової норми та політикою Росії як конкурента, а не як партнера. При цьому слід зауважити, що калькодержателем науково-технічної інформації на НДДКР, виконаних за часів радянської влади, є Москва. Численні спроби державних органів, підприємств і установ України дістати згоду російської сторони на розсекречування деякої науково-технічної документації та спецвиробів позитивного рішення не знайшли.

За даними Міністерства оборони України, наведеними на робочій нараді 25 квітня 2000 року, Військово-технічний комітет при Штабі з координації військового співробітництва країн СНД опрацював та погодив з усіма міністерствами оборони країн—членів СНД механізм надання інформації про скасування (зниження) грифів секретності зразків озброєння і військової техніки, взятих на озброєння до 1992 року. Протягом 1993—2000 років Міністерство оборони України отримало 20 повідомлень на попередні запити, а також переліки зразків ОВТ і технічної документації до них, на які знижено (знято) грифи секретності за 1993—2000 роки. Водночас проблемним залишається отримання інформації про зміну ступеня секретності навчальних посібників, poradників, керівництв, положень та інструкцій з озброєння та військової техніки, їх застосування; з тактики, стратегії, оперативного мистецтва тощо, а також інших нормативних документів, наказів і директив.

Водночас у Російській Федерації розсекречування матеріальних носіїв секретної інформації колишнього СРСР здійснюється на підставі федеральних нормативно-правових документів. Постановою Уряду Російської Федерації від 20 лютого 1995 року затверджено Положення про порядок розсекречування архівних документів Уряду СРСР. У цьому документі відсутні вимоги щодо погодження розсекречування інформації, яка містить міждержавні секрети, з країнами СНД, які підписали мінську угоду від 22 січня 1993 року. Не передбачено й інформування учасників цієї угоди про прийняті рішення щодо розсекречування документів, які містять міждержавні секрети³⁸⁰.

Аналізуючи встановлений у РФ порядок віднесення інформації до державної таємниці та її розсекречування, а також вимоги Положення про порядок розсекречування і продовження строків розсекречування архівних документів Уряду СРСР, можна зробити висновок, що російська сторона вважає своїм державним надбанням інформаційні ресурси (в тому числі такі, що містять міждержавні секрети), які створювалися і використовувалися до укладання мінської Угоди про взаємне забезпечення збереженості міждержавних секретів. Правові норми, що містить цей міжнародний документ стосовно міждержавних секретів, російська сторона поширює тільки на державні секрети, які передаються у рамках співробітництва та створюються в процесі спільних робіт незалежних держав, що підписали зазначену угоду.

Враховуючи вищенаведене стосовно розсекречування секретних інформаційних ресурсів, які залишилися від колишнього СРСР, доцільно вважати їх власністю нашої держави у зв'язку з тим, що вони були створені на державні кошти, і вжити заходів, адекватних діям російської сторони. *Розсекречування, зниження грифів секретності або продовження строків дії цих грифів секретності, встановлених на зазначених носіях секретної інформації, має здійснюватися відповідно до чинних і правових норм України.* Для цього необхідно розробити та ввести в дію нормативно-правові та методичні документи, в яких на підставі науково обґрунтованих критеріїв і методик установити порядок проведення цієї роботи та визначення наукової, історичної, культурної цінності матеріальних носіїв інформації, що підлягають розсекречуванню. При цьому доцільно нагадати, що правила і критерії віднесення документованих носіїв інформації, в тому числі таких, що містять державну таємницю, регламентуються чинним законодавством про Національний архівний фонд і архівні установи³⁸¹. У зв'язку з тим, що Закон України «Про державну таємницю» не містить правових норм регулювання особливостей роботи з розсекречування секретних архівних документів радянських часів, розроблювані нормативно-правові та методичні документи мають визначати порядок участі в цій роботі державних експертів з питань таємниць, заінтересованих державних органів, державних архівних

установ та компетенцію спеціально уповноваженого державного органу для контролю за станом цієї роботи.

Чинне законодавство не визначає правових норм щодо регулювання правовідносин у сфері охорони інформаційних ресурсів, що містять відомості, віднесені до державної таємниці, у зв'язку з переходом до ринкової моделі економіки та приватизацією. Йдеться про реалізацію власником (державою) через відповідні державні органи наданих ним повноважень для встановлення та забезпечення дотримання правового режиму інформаційних ресурсів, що містять відомості, віднесені до державної таємниці, на підприємствах і в установах, які змінили або змінюють форму власності.

Закон України «Про державну таємницю»³⁸² визначає, що державна таємниця підлягає охороні з боку держави, а також, що дія цього закону поширюється на підприємства, установи, організації всіх форм власності. Крім того, цей закон визначає, що «забезпечення охорони державної таємниці відповідно до вимог режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях, діяльність яких пов'язана з державною таємницею, покладається на керівників зазначених органів, підприємств, установ і організацій» (ст.5), а далі встановлює, що «...підприємства, установи, організації мають право провадити діяльність, пов'язану з державною таємницею, після надання їм спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею» (ст. 20).

Аналіз наведених правових норм, що містить Закон України «Про державну таємницю», змушує зробити висновок про те, що ці правові норми не враховують нових суспільних правовідносин, які складаються у процесі роздержавлення власності.

На цей час державні органи, до сфери управління яких належать об'єкти, що приватизуються, та державні органи приватизації, вирішуючи питання про приватизацію підприємств і установ, керуються «Методикою оцінки вартості майна під час приватизації», затвердженою постановою Кабінету Міністрів України від 22 липня 1998 року. Ця методика визначає порядок оцінки цілісного майнового комплексу об'єкта, що приватизується, в тому числі носіїв інформації, які містять державну таємницю (науково-технічна документація, вироби). Передбачається

два варіанти вирішення питання про носіїв секретної інформації.

Перший. Оцінка вартості носіїв інформації, що містить державну таємницю, і включення її до складу вартості цілісного майнового комплексу об'єкта, що приватизується, відбувається за наявності на це згоди державного органу, до сфери управління якого належить об'єкт, що приватизується, та замовника секретних робіт, які виконувалися на цьому об'єкті.

Другий. У разі, коли державний орган, до сфери управління якого належить об'єкт, що приватизується, та замовник секретних робіт не дають згоди на приватизацію носіїв інформації, віднесеної до державної таємниці (науково-технічна документація, вироби), вирішується питання про умови подальшого використання цих носіїв секретної інформації.

Реалізація першого варіанта створює правову колізію щодо права власності на інформацію. Чинне законодавство визначає, що інформація може бути об'єктом права власності як у повному обсязі, так і об'єктом лише володіння, користування чи розпорядження, та регулює правовідносини, пов'язані з переходом права власності від фізичних та юридичних осіб до держави. Власник секретної інформації або її матеріальних носіїв здійснює своє право власності з урахуванням обмежень, установлених в інтересах національної безпеки відповідно до законодавства. І правові норми законодавства про державну таємницю також регулюють тільки правовідносини щодо передавання або вилучення у фізичних та юридичних осіб у власність держави права власності на секретну інформацію або її матеріальні носії.

У першому варіанті зміна права власності на секретну інформацію та її матеріальні носії здійснюється на підставі не правових норм, а вищенаведеної методики — рекомендаційних способів вирішення завдань приватизації.

«Методика оцінки вартості майна під час приватизації» розроблена Фондом держмайна України і затверджена Кабінетом Міністрів України у липні 1998 року на підставі санкціонуючої правової норми, що викладена у Законі України «Про державну програму приватизації» від 12 лютого 1998 року. Цим законом визначено, що наявність у підприємства зобов'язань із мобілізаційної підготовки, збереження державної таємниці не є

підставою для заборони приватизації відповідного об'єкта (ст. 6). Указаною правовою нормою законодавства надано права державним органам, які займаються приватизацією, самим приймати рішення про зміну права власності на секретні інформаційні ресурси та їх носії. Фактично наведений перший варіант створює умови для зміни права власності на секретні інформаційні ресурси не на підставі встановленого законодавством порядку, а на підставі рекомендаційних способів. А це суперечить ст. 41 Конституції України про те, що «право приватної власності набувається в порядку, визначеному законом».

Головна причина такого становища полягає в тому, що чинним законодавством, яке регулює відносини, пов'язані з правом власності на об'єкти інтелектуальної діяльності, не визначено порядку і механізму набуття та реалізації прав держави на об'єкти інтелектуальної власності, створені повністю або частково за рахунок коштів державного бюджету³⁸³, у тому числі на об'єкти інтелектуальної власності, що містять відомості, віднесені до державної таємниці.

У практиці нормотворення у сфері інформаційних відносин в Україні поки що не накопичено необхідного досвіду і це, очевидно, було передумовою того, що законодавець, визначаючи правові норми, спрямовані на регулювання порядку захисту інформації, віднесеної до державної таємниці, у деяких аспектах не відійшов від традиційних підходів, характерних для колишнього СРСР. Досвід розвинутих країн при цьому не враховувався.

Дію Закону України «Про державну таємницю»³⁸⁴ поширено на підприємства, установи й організації всіх форм власності, обов'язок забезпечувати охорону державної таємниці покладено на їх керівників. Така правова норма була визначена підзаконними актами, які діяли в колишньому СРСР, коли всі підприємства належали до державної форми власності. Поширення цієї правової норми у питанні забезпечення охорони інформації, віднесеної до державної таємниці, на керівників підприємств (різних господарських товариств) із недержавною формою власності, якими можуть стати обрані особи без громадянства та іноземці, створює правовий нонсенс.

Запровадження на рівні закону³⁸⁵ дозвільного порядку проведення діяльності, пов'язаної з державною таємницею, є, бе-

зумовно, позитивним досягненням нормотворення у сфері інформаційних відносин. Однак правові норми, що визначають умови надання дозволу на проведення діяльності, пов'язаної з державною таємницею, та на його скасування, не визначають особливостей цієї роботи щодо підприємств, установ і організацій, співвласниками або власниками яких є особи без громадянства та іноземці, а також критеріїв і умов, за якими цим підприємствам і організаціям у видачі такого дозволу може бути відмовлено. Досвід вирішення аналогічних питань у розвинутих країнах із ринковою економікою (США, Франція, Німеччина та ін.) не враховувався.

Так, у Сполучених Штатах Америки секретні роботи на підприємстві не можуть бути розміщені, доки воно не отримає об'єктового допуску³⁸⁶, фактично аналогічного нашому дозволу. У видачі об'єктового дозволу може бути відмовлено в разі, якщо іноземці є власниками шести або більше відсотків акцій підприємства. Об'єктовий допуск у таких випадках може бути виданий лише за умови, якщо до компетентного органу, який видає такий допуск, буде надіслано у двох примірниках протокол засідання співвласників і ради директорів підприємства з рішенням, що іноземні власники акцій не матимуть доступу до секретної інформації і не будуть обіймати посади, які давали б їм змогу негативно впливати на діяльність підприємства під час виконання секретних контрактів.

Нормативно-правові документи США забороняють розміщення секретних замовлень на підприємствах, на яких американська сторона володіє менш як 51% акцій. У всіх таких випадках у видачі об'єктового допуску для виконання секретних робіт надається відмова.

Таким чином, відсутність в інформаційному законодавстві України правових норм, які у повному обсязі залишали б за державою право регулювати порядок формування інформаційних ресурсів, що містять відомості, віднесені до державної таємниці, створюватиме передумови для породження хаосу у цій сфері діяльності. Невизначеність правових норм щодо обмежень у розміщенні на підприємствах з недержавною формою власності замовлень на розробку і виготовлення секретних інформаційних ресурсів створюватиме передумови для витоку та не-

санкціонованого поширення відомостей, віднесених до державної таємниці.

Складною проблемою залишається у державі недосконалість нормативно-правового забезпечення захисту інформаційних ресурсів України, що містять відомості, віднесені до державної таємниці, у процесі міжнародного співробітництва. Аналіз правових норм чинного законодавства, що регламентують правовідносини у цій сфері діяльності, свідчить про те, що розвиток міжнародних зв'язків України значно випереджає розробку й упровадження правових норм, спрямованих на забезпечення ефективного захисту інформаційних ресурсів, віднесених до державної таємниці, як важливої складової інформаційної безпеки держави.

З метою забезпечення гарантій інформаційного суверенітету України чинним законодавством визначено певні правові норми, в тому числі встановлення режиму доступу інших держав до інформаційних ресурсів України³⁸⁷.

Режим доступу інших держав до інформаційних ресурсів, віднесених до державної таємниці, встановлюється правовими нормами, визначеними Законом України «Про державну таємницю»³⁸⁸ та підзаконними актами. Цим законом передбачено, що передання іноземній державі або міжнародній організації інформації, віднесеної до державної таємниці, та її матеріальних носіїв здійснюється на підставі міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, та письмового мотивованого розпорядження Президента України.

В обох випадках Законом України «Про державну таємницю» в редакції 1994 року і в редакції 1999 року передбачається врахування необхідності забезпечення національної безпеки України. Стосовно міжнародних договорів законом 1994 року було встановлено необхідність ратифікації їх Верховною Радою України. Введення правовою нормою закону 1999 року нового порядку, при якому надається згода Верховною Радою України на обов'язковість укладання міжнародних договорів на передання іноземній державі чи міжнародній організації секретної інформації, є більш прийнятним варіантом вирішення цих питань. Він підвищує роль парламентського контролю за експортом секретної інформації, її матеріальних носіїв та знижує можливість колізій, які виникають під час ратифікації вже ук-

ладених договорів. Закон 1999 року встановлює і механізм прийняття рішень: Верховною Радою України — стосовно згоди на обов'язковість міжнародних договорів; Президентом України — щодо письмового мотивованого розпорядження. Такі рішення приймаються, як встановлено законом, лише на підставі пропозицій Ради національної безпеки і оборони України. Розгляд таких пропозицій і Верховною Радою України, і Президентом України значно знижує ймовірність помилок, пов'язаних із захистом національних інтересів у процесі використання секретної інформації та її носіїв у відносинах з іноземними партнерами.

Правовий режим секретної інформації, яка передається (отримується) сторонами у процесі міжнародного співробітництва, визначається договорами про взаємну охорону державних таємниць з урахуванням чинного законодавства сторін та світової практики.

Так, Законом України «Про державну таємницю» встановлено, що передані Україні відомості, що становлять таємницю іноземної держави чи міжнародної організації, охороняються в порядку, передбаченому цим законом, у разі, якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, встановлені інші, ніж передбачені цим законом, правила охорони таємниці іноземної держави чи міжнародної організації, то застосовуються правила міжнародного договору³⁸⁹.

Зміст та порядок підготовки міжнародних договорів про взаємну охорону державних таємниць та порядок оформлення дозволів за розпорядженнями Президента України на передання іншій державі чи міжнародній організації інформації, що становить державну таємницю, та носіїв такої інформації регламентується нормативними документами, затвердженими главою держави.

Актами законодавства та іншими нормативно-правовими документами України визначено порядок контролю і нагляду за дотриманням встановленого режиму передавання іноземній державі чи міжнародній організації секретної інформації або її носіїв, у тому числі в процесі експортного контролю.

Таким чином, правові норми, впроваджені в Україні, дають змогу діяти в процесі міжнародного співробітництва, пов'яза-

ного з використанням секретних інформаційних ресурсів, у межах правового поля держави.

Поряд з цим реалії сьогодення свідчать про те, що державні органи, підприємства, установи й організації не дотримуються правових норм, які регламентують порядок встановлення режиму доступу інших держав до інформаційних ресурсів України, віднесених до державної таємниці. Економічне, наукове, військово-технічне співробітництво та співробітництво в деяких інших сферах, як правило, передбачає використання інформації, що становить державну таємницю, або її матеріальних носіїв, які підпадають під дію таких пунктів Зводу відомостей, що становлять державну таємницю України (ЗВДТ — за станом на 13 квітня 2001 року), як 1.22, 1.23, 1.24, 1.25, які відносять інформацію про дослідження і розробки оборонного та подвійного призначення, деякі зразки озброєнь і військової техніки до державної таємниці. Крім того, відповідно до п.3.3 ЗВДТ зведені відомості про номенклатуру, обсяги та фінансування операцій з експорту озброєнь, військової техніки, окремих стратегічних видів сировини і продукції, а також відомості про військове, військово-технічне та науково-технічне співробітництво з іноземними державами, за винятком тих відомостей, які мають передаватися відповідно до міжнародних зобов'язань, також становлять державну таємницю³⁹⁰. А це означає, що з державами, з якими здійснюється співробітництво з цих питань, мають укладатися угоди про взаємний захист державних таємниць із зобов'язанням іноземних партнерів не розголошувати відомості, віднесені чинним законодавством України до державної таємниці.

У книзі НІСД «Національна безпека України 1994 — 1996 рр.»³⁸¹ наведено такий приклад: «... у 1995 р. ОПК України мав близько 500 прямих договорів із фірмами 23 країн світу». За даними колишнього Держкомсекретів, на початок 1999 р. ОПК України були укладені договори з понад 50 країнами світу. Крім того, з деякими країнами, армії яких оснащені радянськими озброєннями і військовою технікою, підприємства ОПК України здійснювали співробітництво у військово-технічній сфері на підставі договорів, укладених ще колишнім СРСР.

Договори про взаємну охорону державних таємниць у процесі міжнародного співробітництва українською стороною на

початок 1999 року були укладені лише з п'ятьма країнами та з НАТО в рамках співробітництва «Партнерство заради миру». При цьому слід зауважити, що в Україні вживаються певні заходи для приведення міждержавного співробітництва з використанням інформації, віднесеної до державної таємниці, у відповідність до чинного законодавства і міжнародно-правових норм.

Відповідно до оцінок спеціалістів підписана в м. Мінську Угода про взаємне забезпечення збереження міждержавних секретів застаріла. Це підтверджується бажанням країн — членів СНД укласти з Україною окремі угоди з питань захисту таємної інформації. За станом на кінець 2000 року такі угоди були укладені з Республікою Узбекистан (7 жовтня 1999 року), з Російською Федерацією (2 грудня 2000 року) та ін.

Це свідчить про те, що міжнародне економічне, наукове, військово-технічне та інше співробітництво України, пов'язане з використанням інформації, що становить державну таємницю, та її матеріальних носіїв, зі значною кількістю країн здійснюється без встановлення передбаченого міжнародними правовими нормами та чинним законодавством України режиму доступу до відповідних інформаційних ресурсів України.

Зміст режиму доступу та механізм його реалізації має встановлюватися міжнародними договорами України про взаємну охорону державних таємниць, як і передбачено нормативно-правовими актами держави та світовою практикою, та охоплювати:

— зобов'язання сторін здійснювати необхідні заходи для забезпечення охорони державних таємниць, що передаються в процесі співробітництва, всіма суб'єктами господарської та іншої діяльності незалежно від форм власності та підпорядкування відповідно до національного законодавства сторін та взаємно узгоджених критеріїв;

— гарантії щодо виключення передання третій стороні інформації, що становить державну таємницю, її матеріальних носіїв без попередньої письмової згоди сторін та зобов'язання не використовувати отриману інформацію, що становить державну таємницю, та її матеріальні носії з метою, відмінною від встановленої міжнародними договорами або іншими документами про співробітництво;

— процедуру надання доступу громадянам держав, що є сторонами міжнародного договору, до державних таємниць, які передаються;

— порядок взаємного інформування в разі розголошення переданих державних таємниць, а також втрати її матеріальних носіїв;

— зобов'язання про притягнення до відповідальності осіб, винних у розголошенні державних таємниць або втрати їх матеріальних носіїв, згідно із законодавством сторін;

— покладання на підприємства, установи, організації сторін, які безпосередньо здійснюють співробітництво, обов'язків визначати у договорах (контрактах) про передавання (продаж) або створення у процесі спільної роботи носіїв секретної інформації, вимоги режимно-секретного забезпечення на всіх етапах їх виготовлення, передавання (пересилання, транспортування), використання відповідно до строків засекречування інформації, що містять вказані її носії;

— визначення процедури і порядку відшкодування збитків, завданих унаслідок розголошення інформації, що становить державну таємницю, або втрати її матеріальних носіїв;

— порядок вирішення спірних питань охорони державних таємниць;

— порядок досягнення взаємної впевненості, що підприємства, установи, організації кожної із сторін готові забезпечити охорону секретної інформації та її матеріальних носіїв, що передаються (одержуються) відповідно до правових норм, визначених міжнародним договором та законодавством сторін;

— порядок здійснення сторонами контролю за забезпеченням охорони державних (міждержавних) таємниць.

Світова практика організації співробітництва, пов'язаного з обміном, передаванням секретної інформації, свідчить про те, що розвинуті країни вирішують ці питання, керуючись наведеними підходами. Ось деякі приклади.

За повідомленням засобів масової інформації, двостороння українсько-американська робоча група парафувала програми українсько-американських військових контактів та план оборонного співробітництва на 2000 рік, а також домовилася, що найближчим часом будуть укладені відповідні угоди. Для повного розуміння характеру відносин Україна—США слід сказати, що

американська сторона вже на першій зустрічі висунула обов'язкову умову, яка за її вимогами має бути виконана до укладання зазначених угод, а саме: попереднього укладання угоди про взаємний захист секретної інформації, якою сторони будуть обмінюватися в процесі співробітництва.

При цьому нагадаємо, що зі Сполученими Штатами укладена Угода про військово-технічне співробітництво 31 березня 2000 року, яка передбачає лише обмін нетаємною інформацією. У п.10.1 цієї угоди зазначено, що обмін таємною інформацією може здійснюватися тільки після укладання окремої угоди.

У березні 1995 році у м. Брюсселі між Урядом України і НАТО була укладена Угода про безпеку у сфері охорони інформації з обмеженим доступом для обміну інформацією у процесі виконання програми «Партнерство заради миру». Фактичний обмін інформацією з обмеженим доступом, у тому числі з грифами секретності, став здійснюватися лише після взаємного вивчення умов забезпечення охорони цієї інформації. Делегація Офісу безпеки НАТО у звіті за результатами такої перевірки відзначила, що в Україні створена система охорони державної таємниці (процедури одержання, реєстрації, контролю використання та зберігання), яка відповідає світовим стандартам.

Таким чином, зважаючи на викладене, можна зробити такі висновки:

— укладання міжнародних (двосторонніх, багатосторонніх) договорів про взаємну охорону державних таємниць у процесі економічного, наукового, військово-технічного співробітництва, пов'язаного з використанням секретної інформації та її матеріальних носіїв, забезпечує користування інформаційними ресурсами держави на основі рівноправного співробітництва з іншими державами;

— економічне, наукове, військово-технічне співробітництво України, пов'язане з використанням інформації, віднесеної до державної таємниці, та її матеріальних носіїв, без укладання міжнародних договорів про взаємний захист державних таємниць *відводить нашої державі «донорську» роль*; при цьому не передбачено гарантії щодо виключення передавання третій стороні та використання отриманої від України інформації, її матеріальних носіїв на шкоду нашої державі;

— є настійна необхідність подальшого вдосконалення механізму реалізації вимог чинного законодавства до порядку охорони державної таємниці в процесі міжнародного співробітництва, який би забезпечив використання секретних інформаційних ресурсів, їх носіїв на основі рівноправного співробітництва та виключав можливість передавання (продажу) інформаційних ресурсів з обмеженим доступом та їх носіїв без встановлення передбаченого законодавством режиму доступу до них іноземних держав;

— повільно вирішуються питання про підвищення відповідальності державних органів, на яких покладені повноваження здійснювати контрольні і наглядові функції за дотриманням законодавства про державну таємницю в процесі міжнародного співробітництва, в тому числі під час експортного контролю.

Крім того, потребує всебічних досліджень і наукового обґрунтування система правового регулювання захисту науково-технічних інформаційних ресурсів, особливо пов'язаних з фундаментальними та пошуковими дослідженнями й розробками, необхідністю формування національного інформаційного простору, що відповідав би інформаційно-інтелектуальному потенціалові держави та цивілізованому інтегруванню України до світового інформаційного простору не як країни «третього світу».

В умовах неспроможності генерального замовника озброєнь та військової техніки, замовників виробів спеціального призначення фінансувати свої НДДКР та закуповувати навіть одиничні зразки озброєнь, військової техніки і спеціальних виробів застосування лише засекречування як методу захисту отриманих інформаційних ресурсів від несанкціонованого використання тільки стримує економічний розвиток держави та інтегрування її до світового наукового співтовариства. А це лише шкодить інтересам нашої країни.

Для ефективного використання наукоємних традиційно засекречуваних результатів досліджень і розробок за оборонними замовленнями в інтересах впровадження високоефективних наукових розробок, розвитку високотехнологічних вітчизняних виробництв та розвитку міжнародного науково-технічного співробітництва доцільним є розв'язанням таких проблем, як:

— удосконалення механізму засекречування вітчизняної науки, етапів досліджень, розробок, їх результатів, особливо

фундаментальних і пошукових НДДКР, у зв'язку з великою невизначеністю їх кінцевих результатів, багатофункціональністю і багатоваріантністю практичного застосування, а також удосконалення механізму оперативного розсекречування результатів закритих НДДКР, якщо це викликано інтересами розвитку загальної науки та розв'язанням економічних проблем;

— знесення необхідних змін і доповнень до відомчих переліків відомостей, що становлять державну таємницю у сфері науки і техніки, які дають змогу визначати ступінь секретності не тільки відповідних напрямів досліджень і розробок, а й їх окремих етапів та отриманих результатів;

— створення поряд з удосконаленням інституту державної таємниці логічно завершеної ефективно діючої державної інфраструктури захисту інтелектуальної власності, яка виключала б можливість незаконного використання інтелектуальної власності у зв'язку з її комерціалізацією;

— формування ефективного механізму забезпечення реалізації чинних правових норм стосовно договірної системи взаємовигідного міжнародного співробітництва в науково-технічній сфері, яка передбачає чітке визначення зобов'язань іноземних партнерів щодо захисту наданої їм секретної інформації від використання її третіми країнами.

Залишаються ще інші сфери міжнародного співробітництва, пов'язаного з використанням інформації, віднесеної до державної таємниці, які на цей час не врегульовано нормативно-правовими актами України або міжнародними правовими нормами.

Відповідно до програми співробітництва України з НАТО та заходів державних органів, спрямованих на забезпечення її виконання, передбачена адаптація з наступним переходом до озброєнь, які відповідали б світовим стандартам (стандартам НАТО). В Україні стандартизація у сфері досліджень, розробок, виготовлення озброєнь, у тому числі порядку охорони інформації, віднесеної до державної таємниці, що вони містять, значно відстає від потреб сьогодення, не враховує нових реалій, пов'язаних з європейським вибором України. А це також свідчить про те, що розвиток міжнародного співробітництва значно випереджає нормативно-правове регулювання відносин, пов'язаних із захистом інформаційних ресурсів, віднесених до дер-

жавної таємниці у цій сфері діяльності. Співробітництво з НАТО у цій сфері на основі застарілих стандартів є проблематичним.

Не в повному обсязі залишаються врегульованими правові відносини щодо надання права доступу іноземцям до інформації, що становить державну таємницю України. Закон України «Про державну таємницю»³⁹² містить правову норму, яка передбачає надання іноземцям такого права «у виняткових випадках на підставі міжнародних договорів України або письмового розпорядження Президента України з урахуванням необхідності забезпечення національної безпеки України» на підставі пропозицій РНБО України.

У зв'язку з викладеними вимогами цієї правової норми слід привернути увагу до аспектів, пов'язаних із навчанням у військових навчальних закладах України громадян інших країн та діяльністю радників і консультантів іноземних держав та міжнародних організацій у державних органах України. Це світова практика. Водночас в Україні ці процеси здійснюються, як правило, на підставі відомчих домовленостей, що суперечать чинному законодавству. Розв'язання зазначених проблем можна досягти шляхом внесення відповідних доповнень до законодавчої та нормативно-правової бази.

Продовжують прямо чи опосередковано діяти загрози інформації, що становить державну таємницю, та іншій інформації з обмеженим доступом, що є власністю держави, яка використовується зарубіжними представництвами та іншими структурами за кордоном. Передумовою цих загроз є як об'єктивні, так і суб'єктивні чинники. Більшість цих представництв через скрутне економічне становище працюють у непристосованих приміщеннях, немає закритих каналів зв'язку, що створює передумови для витоку інформації, що охороняється. Для вирішення цих питань потрібен значний час і відповідні кошти з державного бюджету.

Другий аспект цього питання пов'язаний із суб'єктивними обставинами, що не потребує надзвичайних інвестицій і тривалого часу, а лише доброї волі і необхідного професіоналізму тих, хто відповідає за дотримання законодавства про державну таємницю у цій сфері діяльності та пов'язані із розробкою і впровадженням відповідних нормативно-правових актів.

Усе це створювало і створюватиме передумови для витоку і розголошення інформації, що становить державну таємницю про тактичні й стратегічні питання зовнішньополітичної і зовнішньоекономічної діяльності, важливі для національної безпеки держави.

Таким чином, недостатньо врегульована правовими нормами діяльність, пов'язана з використанням у процесі міжнародного співробітництва інформаційних ресурсів, що становлять державну таємницю, породжує загрозу не тільки власне в інформаційній сфері, а й у всіх складових національної безпеки, а це може призвести до вкрай негативних наслідків для держави.

Ще однією проблемою у сфері охорони державної таємниці є те, що досі залишається недосконалим механізм реалізації правових норм чинного законодавства про державну таємницю у зв'язку з відсутністю нової Інструкції про режимно-секретну роботу та невизначеністю порядку категоріювання об'єктів, діяльність яких пов'язана з державною таємницею. Більшість вимог нормативного документа, відомого спеціалістам як Інструкція 0126-87 р. застаріла, а деякі з них суперечать вимогам Закону України «Про державну таємницю». Ці недоліки можуть бути усунені лише введенням у дію нової Інструкції про режимно-секретну роботу.

Зазначені проблеми загострюють питання про необхідність вдосконалення правової бази охорони державної таємниці, віднесення якої до цієї категорії безпосередньо пов'язане з інтересами національної безпеки України. Для розв'язання цих проблем було б доцільним передбачити:

а) доповнення чинного законодавства такими правовими нормами:

— про віднесення інформації до державної таємниці у сферах оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки лише на підставі науково обґрунтованих, політичних і соціально-економічних критеріїв, з визначенням державного органу, який затверджує методику віднесення інформації до державної таємниці (такі повноваження доцільно надати Кабінетові Міністрів України — *див. п. 2.3.3*);

— про порядок державної реєстрації інформаційних ресурсів, що становлять державну таємницю, їх накопичення, зберігання і використання та взаємодію органів державної реєстрації

цих ресурсів з державними експертами з питань таємниць та спеціально уповноваженим органом державної влади у сфері охорони державної таємниці;

— про порядок охорони державної таємниці у зв'язку з переходом до ринкової моделі економіки, на підприємствах і установах, які змінюють форму власності, з визначенням критеріїв обмежень щодо надання дозволу для здійснення діяльності, пов'язаної з державною таємницею, підприємствам і організаціям, власниками яких повністю або частково є особи без громадянства та іноземні фізичні та юридичні особи;

— про порядок зміни форми власності на інформаційні ресурси, що становлять державну таємницю, в процесі приватизації — відповідно до вимог ст.41 Конституції України про те, що право приватної власності набувається в порядку, визначеному законом;

— про порядок охорони державної таємниці у випадках, якщо інформація віднесена до державної таємниці та її матеріальні носії включаються у сферу товарних відносин не тільки у межах країни, а й у процесі міжнародного співробітництва й одночасно становить і комерційну таємницю;

— про порядок здійснення державного контролю за дотриманням законодавства про державну таємницю на підприємствах і в організаціях з недержавною формою власності з визначенням для цього повноважень місцевих державних органів;

б) розробити та в установленому порядку ввести в дію міжнародні та внутрішні нормативно-правові документи:

— міжнародні (двосторонні, багатосторонні) договори про взаємну охорону державних таємниць з державами, з якими здійснюється економічне, наукове, військове, військово-технічне співробітництво, пов'язане з використанням секретної інформації та її матеріальних носіїв;

— про порядок охорони державної таємниці та забезпечення режиму секретності в закордонних представництвах України; окремим документом визначити цей порядок у військових формуваннях України, що перебувають за кордоном;

— про порядок охорони державної таємниці у сфері озброєнь у зв'язку з переходом до стандартизації озброєнь за світовими стандартами;

— про режим доступу до інформаційних ресурсів України радників і консультантів іноземних держав, міжнародних організацій, що працюють у державних органах, з визначенням порядку дотримання встановлених законодавством обмежень щодо їх доступу до інформації, віднесеної до державної таємниці;

— про порядок розсекречування, зниження грифів секретності та продовження строків дії цих грифів секретності, встановлених на інформаційних ресурсах у радянські часи.

4.2.2. Проблеми у сфері захисту інформації з обмеженим доступом, що не становить державної таємниці

Аналіз інформаційного законодавства України щодо регулювання суспільних відносин, пов'язаних з захистом інформації з обмеженим доступом, що не становить державної таємниці, дає багато свідчень того, що ця сфера на правовому рівні залишається неврегульованою.

Якщо стосовно державної таємниці йдеться про вдосконалення законодавчої та нормативної бази, то у сфері інформаційної діяльності, пов'язаної з конфіденційною та іншою передбаченою законом таємницею — про подолання правового хаосу та усунення колізій між законодавчими актами, які не дають можливості не тільки забезпечувати ефективний захист інформаційних ресурсів, а взагалі встановити цивілізовані інформаційні відносини. Ця проблема вкрай складна. У світовій практиці її розв'язання потребувало кількох десятиріч. Безумовно, за роки незалежності нашої держави розв'язати всі проблеми інформаційних відносин, зокрема, захисту інформаційних ресурсів, що підлягають охороні з боку держави, неможливо.

На сьогодні в Україні створена певна законодавча база, яку можна віднести до інформаційної галузі. Для більш повного уявлення про проблеми правового регулювання інформаційних відносин, пов'язаних з захистом інформаційних ресурсів, нагадаємо основні акти законодавства:

— закони, які безпосередньо стосуються інформації як об'єкта правовідносин та процесу інформатизації: «Про інформацію», «Про науково-технічну інформацію», «Про державну таємницю», «Про захист інформації в автоматизованих системах»,

«Про концепцію Національної програми інформатизації», «Про Національну програму інформатизації»;

— закони, які регламентують суспільні відносини, що виникають в інформаційній сфері, стосовно масового поширення: «Про друковані засоби масової інформації (пресу) в Україні», «Про телебачення та радіомовлення», «Про інформаційні агентства», «Про систему суспільного телебачення і радіомовлення», «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації», «Про державну підтримку засобів масової інформації та соціальний захист журналістів», «Про зв'язок», «Про бібліотеки і бібліотечну справу», «Про національний архівний фонд і архівні установи», «Про музеї і музейну справу», «Про рекламу» та ін.;

— закони, які регулюють різноманітні суспільні відносини, що стосуються власності, об'єктом яких може бути інформація: «Про власність», «Про авторське право і суміжні права», «Про підприємства в Україні», «Про підприємництво», «Про Національну програму приватизації», «Про охорону прав на винаходи та корисні моделі», «Про охорону прав на промислові зразки», «Про внесення змін і доповнень до деяких законодавчих актів України щодо охорони інтелектуальної власності», «Про банки та банківську діяльність», «Про господарські товариства», «Про обмеження монополізму та недопущення недобросовісної конкуренції в підприємницькій діяльності», «Про захист від недобросовісної конкуренції» та деякі ін.;

— закони, які містять правові норми, що регулюють окремі питання захисту інформації про особу (персональні дані): «Основи законодавства України про охорону здоров'я», «Про статус і соціальний захист громадян, які постраждали внаслідок Чорнобильської катастрофи», «Про запобігання захворюванню на синдром набутого імунodefіциту (СНІД) та соціальний захист населення», «Про органи реєстрації актів цивільного стану», «Про всеукраїнський та місцеві референдуми», «Про міліцію», «Про прокуратуру», «Про нотаріат», «Про страхування», «Про державний реєстр фізичних осіб—платників податків та інших обов'язкових платежів» та ін.;

— правові норми, що містять кодифіковані акти законодавства та міжнародно-правові акти, до яких приєдналася Україна, спрямовані на врегулювання відносин в інформаційній сфері.

Крім того, розглядаючи інформаційне законодавство, потрібно врахувати, що в державі триває робота, спрямована на створення законодавчої бази.

На розгляді у Верховній Раді України перебувають проекти законів: «Про інформаційний суверенітет та інформаційну безпеку», «Про єдиний державний реєстр фізичних осіб та порядок їх реєстрації», «Про радіочастотний ресурс України», «Про захист суспільної моралі», «Про внесення змін до Закону України «Про рекламу». Підготовлено до подання у Верховну Раду України проект Закону України «Про концепцію розвитку телерадіоінформаційного простору України». Окрім того, у процесі розроблення перебувають проекти Законів України «Про захист персональних даних», «Про контроль стану інформаційної безпеки в мережах передачі даних», «Про електронний документ та електронний документообіг», «Про легітимність електронного підпису», «Про національні інформаційні ресурси» та ін.

Як чинні акти законодавства, так і ті, що перебувають на розгляді у Верховній Раді України та розробляються, не забезпечують створення комплексної (загальної) системи захисту інформації та подолання колізії правових норм. Зупинимося лише на найпринциповіших проблемах.

Чинним законодавством не надається повне юридичне тлумачення понять «інформація», «інформаційний ресурс». Так, у Законі України «Про інформацію»³⁹³ сказано: *«Ніщ інформацією цей закон розуміє документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі»*. *«Інформаційний ресурс»*, — як це трактує Закон України «Про Національну програму інформатизації»³⁹⁴, — сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо). Таке визначення «інформації», «інформаційного ресурсу» як об'єкта товарних відносин надто вузьке, не враховує їх феномену, який включає такі складові їхньої характеристики: «інформація», «інформаційний ресурс» як продукт інформаційної діяльності, як державний та національний ресурс, як ідея, як об'єкт права власності фізичних, юридичних осіб та держави.

Аналіз правових норм чинного законодавства свідчить про те, що регулювання правовідносин, пов'язаних із формуван-

ням, використанням і захистом інформаційних ресурсів (інформації), здійснюється на підставі окремих традиційних норм майнового права. Відсутність чіткого повного юридичного визначення понять «інформація», «інформаційний ресурс» призвело до того, що в кримінальному та адміністративному праві відсутні науково обгрунтовані юридичні тлумачення всього спектру правопорушень в інформаційній сфері, що є головною причиною того, що ці галузеві інститути законодавства не в повному обсязі передбачають відповідні правові санкції за цей спектр правопорушень.

На правовому рівні не визначено й основні вимоги до ціноутворення на інформаційні ресурси як товар у процесі купівлі-продажу. Сама лише договірна система встановлення ціни на інформаційну продукцію, як це передбачено законами України «Про інформацію» і «Про науково-технічну інформацію», в умовах інформатизації всіх сфер діяльності суспільства, не забезпечуватиме потреб формування інформаційного ринку. Насамперед це стосується науково-технічної інформації. Без правового регулювання ринкових відносин в інформаційній сфері уявляється проблематичним захист інформаційних ресурсів держави, пов'язаних з перспективними дослідженнями і розробками, наукоємними новітніми технологіями та іншою важливою інформацією, яка, як правило, має відповідний ступінь обмеження доступу. Нові явища, пов'язані з елементами «чорного ринку» інформації, який вже формується, є яскравим підтвердженням наведеного висновку.

Чинне інформаційне законодавство містить поняття і категорії, а також правові норми, які неоднозначно тлумачаться, має місце розбіжність у їх розумінні. Слід зазначити, що юридично не з'ясовані і концептуально не узгоджені поняття, категорії та правові норми переносяться прибічниками тієї чи іншої точки зору до тексту законопроектів, а це загрожує надалі впровадженням у дію законів та підзаконних актів, що суперечать один одному та вже існуючому законодавству щодо інформаційної сфери. Усе це створювало і створюватиме передумови для правового хаосу в інформаційній сфері, пов'язаній із захистом інформаційних ресурсів з обмеженим доступом.

Законом України «Про інформацію»³⁹⁵ встановлено, що інформація з обмеженим доступом поділяється на конфіденційну і

таємну. Нагадаємо, що відповідно до чинного законодавства в Україні близько двох десятків різних видів таємної інформації (крім державної таємниці) та кілька видів конфіденційної інформації.

Найбільш принциповим питанням щодо інформації з обмеженим доступом, що не становить державної таємниці, є необхідність законодавчого визначення правового режиму кожного виду такої інформації (див. п.п. 2.2. і 3.2). Лише нагадаємо, що правовий режим інформації та межі його дії є підґрунтям для встановлення інформації взаємодії між державною владою, особою і суспільством, важливим інструментом для формування необхідного балансу між потребою у вільному обміні інформацією і припустимими обмеженнями на її поширення. Без законодавчого визначення правового режиму кожного виду інформації з обмеженим доступом, що не становить державної таємниці, є проблематичним розроблення і впровадження ефективно діючих механізмів забезпечення права власності на відповідні інформаційні ресурси, а також права володіти, користуватися, розпоряджатися ними.

У зв'язку з цією проблемою виникають і інші запитання.

Який гриф обмеження доступу або обмежувальну позначку треба надавати матеріальним носіям кожного виду інформації з обмеженим доступом? При цьому слід враховувати, що цей перелік містить інформацію, яка є власністю держави, інформацію, яка є власністю фізичних і юридичних осіб, а також інформацію про фізичних і юридичних осіб, яка в установленому законом порядку збирається і накопичується у державних органах для виконання функцій державного управління.

Гриф обмеження доступу є важливим елементом правового режиму інформації з обмеженим доступом і має встановлюватися на рівні правових норм.

У колишньому СРСР для службової та військової таємниці був встановлений гриф обмеження доступу «секретно», іншій інформації з обмеженим доступом надавався гриф обмеження доступу «для службового користування». Законодавством Російської Федерації інформація з обмеженим доступом поділяється на державну таємницю і конфіденційну інформацію. Усім видам конфіденційної інформації, як це встановлено законодавством Росії³⁹⁶, надається гриф «конфіденційно». На рівні правових норм

визначено порядок встановлення грифів обмеження доступу до інформації з обмеженим доступом і в інших країнах, у тому числі в США, Німеччині, Франції, Китаї та ін.

Зважаючи на те, що в Україні зміст правового режиму інформації з обмеженим доступом чинним законодавством встановлено не в повному обсязі, а визначені лише його фрагменти, автори нових проектів законів і підзаконних актів поняття і норми чинного законодавства використовують довільно, відповідно до свого розуміння та на свій розсуд.

Так, згідно зі ст. 30 Закону України «Про інформацію»³⁹⁷ поняття «конфіденційна інформація» не поширюється на інформацію з обмеженим доступом, що становить іншу передбачену законом таємницю і є власністю держави. Як визначено у другому і третьому абзацах цієї статті, конфіденційна інформація — це відомості, якими володіють, користуються або поширюють окремі фізичні чи юридичні особи, та інформація професійного, ділового, виробничого, банківського, комерційного й іншого характеру, одержана на власні кошти громадянами та юридичними особами або є предметом їхнього інтересу. Така інформація поширюється за їх бажанням, вони самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему і способи захисту. А такі підзаконні акти, як державний стандарт України ДСТУ 3396.2-97, введений у дію у січні 1997 року, та Інструкція, затверджена Кабінетом Міністрів України у листопаді 1998 року³⁹⁸, поняття «конфіденційна інформація» поширюють на інформацію з обмеженим доступом, що не становить державної таємниці і є власністю держави. За цією Інструкцією, всім матеріальним носіям усіх видів інформації з обмеженим доступом, що не становить державної таємниці, які є власністю держави, надається гриф обмеження доступу «для службового користування».

Наведені правові норми, які дають право окремим фізичним чи юридичним особам самостійно встановлювати правовий режим інформації, і те, що Держстандартом і Кабінетом Міністрів України поняття «конфіденційна інформація» поширено на всі види інформації з обмеженим доступом, що не становить державної таємниці, зумовлено тим, що ст. 30 закону³⁹⁹ фактично не розмежовує конфіденційну і таємну інформацію, існують

суперечності як у самій статті, так і з іншими статтями цього закону.

Приміром, визначення таємної інформації базується на тому, що її розголошення завдає шкоди особі, суспільству, державі. Окрема фізична особа також встановлює режим обмеження доступу, включаючи інформацію до категорії конфіденційної, керуючись тим, що її несанкціоноване розголошення може завдати шкоди цій особі. Так само згідно зі змістом цієї статті і державні юридичні особи, які володіють відповідною інформацією на правах повного господарського володіння або оперативного управління, можуть відносити таку інформацію до категорії конфіденційної, в тому разі, якщо її розголошення може завдати шкоди суспільним інтересам, цій юридичній особі чи державі.

Стаття 28 Закону України «Про інформацію»⁴⁰⁰ встановлює, що «режим доступу до інформації — це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації». Тобто закон охороняє як таємну, так і конфіденційну інформацію. Виходячи з цього твердження про захист таємної інформації за допомогою закону, а конфіденційної — засобами власника, можна зробити висновок, що це правовий нонсенс.

Наступним важливим аспектом є віднесення інформації до категорій конфіденційної й іншої передбаченої законом таємниці та встановлення режиму доступу, на підставі права власності на інформацію. До категорії конфіденційної відносять інформацію фізичні і юридичні особи і встановлюють режим доступу, керуючись абсолютним правом власності з метою захисту своїх інтересів. Держава як власник інформації, створеної на кошти державного бюджету⁴⁰¹, відносить інформацію до категорії таємної, керуючись повноваженнями захищати суспільні інтереси для запобігання шкоди особі, суспільству, державі⁴⁰². А це означає фактично позбавлення держави права власності на інформацію, що суперечить і нормам цього закону, і Конституції України.

Не можуть вважатися обґрунтованими і такі норми чинного законодавства, які встановлюють різні вимоги до захисту таємної і Конфіденційної інформації, а саме: захист таємної інформації передбачено з моменту її виникнення, якщо закон визнає

таку інформацію таємною; захист конфіденційної інформації здійснюється з моменту прийняття такого рішення власником інформації. Відсутність визначення на рівні закону переліку видів інформації, що становить «іншу передбачену законом таємницю»⁴⁰³, та віднесення до компетенції «відповідних державних органів»⁴⁰⁴ визначення порядку обігу таємної інформації та її захисту створюватиме передумови для протиправного обмеження права на інформацію.

Не можна вважати обґрунтованим віднесення інформації до категорії конфіденційної та впровадження засобів її захисту на підставі *інтересу до неї фізичної чи юридичної особи* у зв'язку з тим, що такий інтерес може мати і кримінальну спрямованість.

Чинне законодавство, яке регулює відносини у сфері інформаційної діяльності, пов'язаної з інформацією з обмеженим доступом, що не становить державної таємниці, містить й інші суперечності та концептуально неузгоджені поняття і категорії. Найбільшою з них є відсутність чіткого визначення таких правових норм, як режим доступу до інформації з обмеженим доступом та правовий режим такої інформації. Ці правові норми є визначальними для забезпечення захисту інформаційних ресурсів з обмеженим доступом. Без розв'язання на правовому рівні цих питань, захист усіх видів інформації, яка належить до категорії інформації з обмеженим доступом, що не становить державної таємниці, є проблематичним.

Для врегулювання відносин в інформаційній сфері стосовно захисту інформації з обмеженим доступом, що не становить державної таємниці, тобто конфіденційної та «іншої передбаченої законом таємниці», доцільно законодавчо чітко визначити правовий режим інформації з обмеженим доступом та його складової — режим доступу (*див. п. 3.2*).

Крім того, слід підкреслити: встановлюючи на рівні закону правовий режим інформації з обмеженим доступом, що не становить державної таємниці, слід усунути суперечності та непорозуміння у чинних актах законодавства, якими не встановлено межі дії правового режиму кожного виду такої інформації.

Так, ст. 46 Закону України «Про інформацію» встановлено: «Не підлягають розголошенню відомості, що становлять державну або іншу передбачену законом таємницю»⁴⁰⁵. Від указа-

них видів таємної інформації законодавець чомусь відмежовує лікарську таємницю, таємницю грошових вкладів, прибутків від підприємницької діяльності, усиновлення, листування, телефонних розмов і телеграфних повідомлень, фактично виключаючи ці види таємниці з категорії таємної інформації. У ст. 47, що встановлює відповідальність за порушення законодавства про інформацію, також не передбачено відповідальність за розголошення конфіденційної інформації, крім інформації про особисте життя громадян. Слід усунути розбіжності щодо меж дії правового режиму інформації стосовно військової, банківської таємниці, таємниці страхування, адвокатської таємниці, таємниці нотаріальних дій та ін.

Розглянемо проблеми правового регулювання окремих видів таємниць, передбачених законодавством.

На перше місце доцільно винести проблеми, пов'язані з забезпеченням захисту *таємниці особистого життя людини, даних про особу (персональних даних)*.

Правові норми, спрямовані на захист інформації про особисте життя громадянина, містить Конституція України, закони України «Про інформацію», «Про державний реєстр фізичних осіб — платників податків та інших обов'язкових платежів», Кримінальний кодекс України та ін.

Крім того, Україна приєдналася до Конвенції про захист (прав) фізичних осіб у зв'язку з автоматизованою обробкою персональних даних, підписаної державами—членами Ради Європи у Страсбурзі у січні 1991 року⁴⁰⁶. До робочої групи Консультативного комітету Ради Європи, яка розглядала питання захисту персональних даних у зв'язку з автоматизованою обробкою цих даних, було включено і представника України.

Метою цієї конвенції є захист на території кожної держави—учасниці прав і основних свобод кожної фізичної особи, незалежно від її національності та місця проживання, особливо права на захист конфіденційності приватного життя у зв'язку з автоматизованою обробкою її персональних даних.

За конвенцією, її учасницями є держави — члени Ради Європи, які підписали конвенцію, і держави, що приєдналися до неї, але не входять до Ради Європи. Для держав, що приєднуються, конвенція набуває чинності через три місяці після подання акта про приєднання.

Згідно з вимогами конвенції, кожна держава-учасниця і кожна держава, яка приєдналася, зобов'язані до набуття чинності конвенції привести національне законодавство у відповідність до правових норм, що містить цей міжнародно-правовий акт; призначити один або більше уповноважених органів з чітким розмежуванням їх повноважень для виконання завдань, визначених конвенцією; розробити і впровадити механізм реалізації правових норм конвенції і національного законодавства, який має включати організаційні, нормативно-правові та інженерно-технічні заходи, спрямовані на забезпечення гарантій безпеки персональних даних; чітко визначити механізм забезпечення прав людини та покарання за порушення норм національного законодавства у питанні захисту конфіденційності приватного життя, у зв'язку з автоматизованою обробкою персональних даних; на рівні законодавства визначити винятки і обмеження у виконанні правових норм конвенції і то лише пов'язаних із захистом національної безпеки, фінансової стабільності держави, вирішенням завдань боротьби з кримінальною злочинністю. Крім того, конвенція визначає порядок виконання її вимог у процесі передавання персональних даних через кордони, взаємодії держав, що взяли на себе зобов'язання виконувати конвенцію, та звітності цих держав перед Радою Європи. Для безпосереднього керівництва в роботі Комітетом Міністрів Ради Європи у лютому 1995 року прийнято Рекомендації «Захист персональних даних у сфері телекомунікаційних послуг і особливо телефонних послуг»⁴⁰⁷.

Відповідно до Закону України «Про інформацію»⁴⁰⁸, «основними даними про особу (персональними даними) є: національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження». Закон України «Про державний реєстр фізичних осіб—платників податків та інших обов'язкових платежів»⁴⁰⁹ із персональних даних, що входять до Державного реєстру, виключає передбачені Законом України «Про інформацію» дані про національність, освіту, сімейний стан, релігійність, стан здоров'я та додатково включає відомості про місце основної роботи, види сплачуваних податків та інших обов'язкових платежів. Будь-яких обмежень щодо автоматизованої обробки перелічених даних про особу, чинне законодавство не передбачає, що суперечить правовим нормам

конвенції⁴¹⁰, якою встановлено, що автоматизованій обробці підлягають лише дані, які дають змогу ідентифікувати особу. При цьому визначено, що не підлягають автоматизованій обробці персональні дані про расове походження, політичну орієнтацію, релігійні та інші переконання, про стан здоров'я, сексуальну поведінку, притягнення до кримінальної відповідальності, якщо національне законодавство не забезпечує гарантії захисту цих відомостей.

Чинне законодавство України встановлює певні гарантії захисту персональних даних кожного громадянина України як важливої складової забезпечення прав і свобод людини. Конституцією України проголошено⁴¹¹, що іноземці та особи без громадянства, що перебувають на території України на законних підставах, користуються тими самими правами і свободами, як і громадяни України. Однак будь-яких гарантій захисту персональних даних іноземців та осіб без громадянства, як це вимагає конвенція⁴¹², не встановлено.

Перелічені суперечності чинного законодавства України і правових норм, що містить конвенція, підлягають усуненню на рівні актів законодавства держави.

Відповідно до Закону України «Про державний реєстр фізичних осіб — платників податків та інших обов'язкових платежів»⁴¹³ «відомості Державного реєстру є інформацією з обмеженим доступом». Конституція України⁴¹⁴ визначає відомості про громадянина «як конфіденційну інформацію про особу». Законом України «Про інформацію»⁴¹⁵ визначено, що «інформація про особу охороняється Законом». Певні дані про особу містять таємниці досудового слідства, адвокатська таємниця, лікарська таємниця, таємниця усиновлення та ін. Отже, потребує законодавчого визначення, до якого виду інформації з обмеженим доступом належить інформація про особу (персональні дані), а саме: до конфіденційної інформації чи до «іншої передбаченої законом таємниці»?

Принциповим аспектом, пов'язаним з персональними даними, є визначення власника і розпорядника відомостей про особу. Законом України «Про інформацію»⁴¹⁶ встановлено, що «інформація може бути об'єктом права власності як у повному обсязі, так і об'єктом лише володіння, користування чи розпорядження». Конституцією України⁴¹⁷ встановлено, що без згоди

особи збирання, зберігання, використання та поширення конфіденційної інформації про цю особу не допускається, крім випадків, визначених законом. А це означає, що конституційною нормою право абсолютної власності на відомості про свої персональні дані надані особі, яка відповідно до законодавства⁴¹³ на свій розсуд встановлює режим доступу і способи охорони цієї інформації. А наявність у частині другій ст. 32 Конституції України спеціального обмовлення, «крім випадків, визначених законом», на які не потрібна згода особи, дає підстави для висновку, що в таких випадках інформація може бути і відкритою у зв'язку з тим, що жодних обмежень у подальшому для її використання і зберігання не встановлюється. Правові норми Конвенції про захист (прав) фізичних осіб⁴¹⁹ покладають на державу обов'язок забезпечити захист персональних даних у зв'язку з тим, що інформація про особу збирається незалежно від її волі в інтересах виконання функцій державного управління. Норми чинного законодавства України з цих питань потребують уточнень на рівні актів законодавства і приведення їх у відповідність до вимог цієї конвенції⁴²⁰.

Частиною третьою ст. 32 Конституції України встановлено обмеження права на ознайомлення особи з інформацією про себе, яка є державною або іншою захищеною законом таємницею. Зміст цієї правової норми фактично забороняє знайомитися особам з інформацією про себе, що становить зміст адвокатської, банківської, комерційної таємниці, таємниці усиновлення та ін. А це є елементом необґрунтованого обмеження прав людини.

Рекомендації Комітету Міністрів Ради Європи «Захист персональних даних у сфері телекомунікаційних послуг і особливо телефонних послуг»⁴²¹ пропонують урядам держав забезпечити відображення в національних законах і застосувати на практиці положення, викладені у цих рекомендаціях, та керуватися ними всім суб'єктам, які надають телекомунікаційні послуги. Чинне законодавство України не містить правових норм, спрямованих на комплексне забезпечення захисту персональних даних у процесі виконання Національної програми інформатизації. Обов'язок державних органів та організацій, органів місцевого самоврядування, інформаційні системи яких містять інформацію про громадян, вживати, як це передбачено законом⁴²², заходів

для запобігання несанкціонованого доступу до інформації про цих громадян, а цього явно недостатньо.

Приведення законодавства України у відповідність до міжнародних правових норм, встановлених конвенцією⁴²³ і рекомендаціями⁴²⁴ щодо захисту персональних даних, сприятиме формуванню і розвитку демократичного суспільства, входженню України до світового інформаційного простору на основі рівноправного співробітництва з іншими державами.

Досвід розвинутих країн свідчить про те, що в умовах ринкової моделі економіки важливе значення має захист інформації, що становить комерційну таємницю. Виникнення нових суспільних відносин, характерних для ринкової економіки, в тому числі пов'язаних з конкуренцією, потребують виконувати в повному обсязі проголошені Конституцією України⁴²⁵ обов'язки держави бути гарантом правового регулювання цих відносин, суб'єктом яких є не тільки фізичні та юридичні особи, а й держава.

Чинні акти законодавства України містять певні правові норми, спрямовані на регулювання правовідносин, пов'язаних з комерційною таємницею. Закон України «Про підприємства в Україні»⁴²⁶ визначає поняття «комерційна таємниця» як відомостей, що не становлять державної таємниці, пов'язаних з виробництвом, технологічним процесом, управлінням, фінансами та іншою діяльністю підприємства, розголошення (передання, витік) яких може завдати шкоди його інтересам, а також, що склад і обсяг відомостей, які становлять комерційну таємницю підприємства, визначаються його керівником. У серпні 1993 року Кабінетом Міністрів України затверджено Перелік відомостей, що не становлять комерційної таємниці⁴²⁷. Кримінальний кодекс України містить правові санкції за скоєні злочини проти індивідуальної власності громадян, а саме:

— незаконне збирання з метою використання відомостей, що становлять комерційну таємницю (розглядається як промислове шпигунство);

— умисне розголошення комерційної таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною чи службовою діяльністю, якщо воно вчинене з корисливих або інших особистих мотивів і завдало значної шкоди суб'єктові підприємницької діяльності.

Це основні правові норми, що регламентують правовідносини у сфері діяльності, пов'язаної з комерційною таємницею. Правовідносини, пов'язані з охороною авторських прав, прав на винаходи, промислові зразки, корисні моделі, регулюються окремими законами⁴²⁸. Аналіз правового регулювання відносин у цій сфері свідчить, що інститут комерційної таємниці є недосконалим, не забезпечує ні захисту інформації, що містить комерційну таємницю, ні інтересів фізичних, юридичних осіб і держави та й у правовому відношенні має певні суперечності. Найбільш принциповими недоліками чинного законодавства про комерційну таємницю є те, що:

— не визначено правового режиму інформації, що містить комерційну таємницю, і його складової — режим доступу. Без визначення на рівні закону правового режиму цього виду таємниці та режиму доступу до неї забезпечити захист комерційної таємниці неможливо;

— правові норми чинного законодавства необґрунтовано виключають із правовідносин, пов'язаних з комерційною таємницею, державу, не враховуючи, що інформація та її матеріальні носії, створені на кошти державного бюджету, є власністю держави. При цьому не встановлено правових норм захисту інтересів держави у сфері діяльності, пов'язаної з комерційною таємницею, в тому числі інформаційно-інтелектуальних ресурсів, створених повністю або частково за рахунок коштів державного бюджету;

— визначення поняття «комерційна таємниця» як відомостей, які не становлять державної таємниці, суперечить законам України «Про державну таємницю»⁴²⁹, «Про науково-технічну інформацію»⁴³⁰, іншим актам законодавства⁴³¹ та підзаконним актам, на підставі яких інформація, що становить державну таємницю, та її матеріальні носії включаються до сфери товарних відносин. У цій сфері діють комерційні та конкурентні норми і правила. А це означає, що інформація, віднесена до державної таємниці, та її матеріальні носії одночасно можуть бути і комерційною таємницею. Для передавання, продажу такої інформації та її матеріальних носіїв іноземним державам чинне законодавство встановлює відповідні обмеження;

— не досить гнучкий механізм прийняття рішень про можливість передавання, продажу іноземній державі інформацій-

них ресурсів, що становлять державну таємницю, та її матеріальних носіїв, які одночасно становлять і комерційну таємницю, на основі рівноправного міжнародного співробітництва, якщо це викликано необхідністю забезпечення стабілізації економічного, фінансового становища та життєво важливих інтересів держави.

Для передавання, продажу іноземній державі чи міжнародній організації інформації, що містить державну таємницю, та її матеріальних носіїв потрібна наявність міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, або письмове мотивоване розпорядження Президента України⁴³². Для отримання таких рішень потрібен значний час, а це створює передумови для ігнорування правових норм чинного законодавства про державну таємницю на користь комерційних інтересів. Такі рішення часто приймаються державними органами, а інколи й керівниками підприємств, що не мають на це передбачених законодавством повноважень.

Недоліки і суперечності правових норм чинного законодавства про комерційну таємницю та концептуальну неузгодженість їх з правовими нормами законодавства про державну таємницю можна усунути лише на основі актів законодавства. При цьому слід чітко законодавчо визначити поняття «комерційна таємниця» та її співвідношення з «державною таємницею» з урахуванням того, що «державна таємниця» — поняття значно ширше, ніж «комерційна таємниця», і включає такі аспекти. *По-перше*, державна таємниця охоплює відомості, які не включаються до сфери товарних відносин і не є предметом купівлі-продажу. *По-друге*, до державної таємниці можуть належати і відомості, що мають ринкову вартість і є предметом купівлі-продажу (об'єкти інтелектуальної власності, озброєння і військова техніка, що містять відомості, віднесені до державної таємниці).

Таким чином, правовідносини щодо регулювання суспільних відносин у процесі діяльності, пов'язаної з інформацією з обмеженим доступом, що не становить державної таємниці, фактично є «білою плямою» в інформаційному законодавстві України. Відсутність розмежування конфіденційної та «іншої передбаченої законом таємниці», чіткого визначення правового режиму цих видів інформації, концептуальна неузгодженість

підходів до викладення норм, понять та категорій, ігнорування реалій сьогодення щодо розбудови держави, розвитку суспільства та міжнародного співробітництва — все це робить правові норми чинного законодавства про інформацію з обмеженим доступом, що не становить державної таємниці, непридатними для практичного застосування. Враховуючи, що інформаційні ресурси, які підлягають охороні з боку держави, стосуються усіх сфер забезпечення національної безпеки, життєво важливих інтересів особи, суспільства і держави, зволікання з розв'язанням зазначених проблем може призвести до негативних наслідків, які навіть важко передбачити.

Основою для забезпечення вираженої державної політики мають бути акти законодавства — в цьому корені правової держави. У демократичних країнах державна політика реалізується тільки у правових формах, які відповідають Основному Закону держави. Сформувавши проголошену державою систему охорони інформації⁴³³ можна лише створенням необхідної законодавчої бази і вдосконаленням чинного законодавства з питань захисту інформації.

Автору дослідження відомі три варіанти концепцій реформування інформаційного законодавства, зокрема Концепція реформування законодавства України у сфері суспільних інформаційних відносин, яка була прийнята за основу 6 жовтня 2000 року урядовою комісією з питань інформаційно-аналітичного забезпечення органів виконавчої влади (Інтернет: <http://mndc.naiu.kyiv.ua>). Цей проект концепції підтримано у різних органах влади і серед наукової громадськості. Метою реформування інформаційного законодавства є систематизація норм права до найвищої форми, до якої належить кодифікація. Інформаційний кодекс, проект якого запропоновано розробити, має забезпечити правове врегулювання суспільних відносин в інформаційній сфері та інформаційну безпеку всіх сфер життєдіяльності суспільства, а також виправити недоліки чинного законодавства в сфері інформації та уточнити його положення, в тому числі відповідні положення Конституції України, з метою усунення двозначних тлумачень деяких правових норм та виключити можливості для подальших непорозумінь. Кодифікація правових норм інформаційного законодавства передбачає врахування світового досвіду, а це створюватиме передумови для

цивілізованого входження України в світовий інформаційний простір.

Підтримуючи ідею розроблення Інформаційного кодексу і враховуючи, що для систематизації норм інформаційного права потрібен тривалий час, вважаю, що доцільно йти шляхом правового вдосконалення інституту державної таємниці, створення законодавчої та нормативно-правової бази захисту інформації з обмеженим доступом, яка не становить державної таємниці.

Правовий режим інформації, зокрема режим доступу до конкретної категорії інформації з обмеженим доступом, можна визначити лише правовими нормами актів законодавства про відповідні категорії такої інформації. Для цього потрібно як внести відповідні доповнення до чинного актів законодавства, так і розробити та ввести в дію нові закони і підзаконні акти. Потрібно терміново розробити і прийняти такі закони, як: «Про інформацію з обмеженим доступом» та «Про захист інформації».

Так, Закон України «Про інформацію з обмеженим доступом» має врегулювати відносини стосовно всіх видів «конфіденційної та іншої передбаченої законом таємниці». Цей закон має визначити термінологію стосовно інформації з обмеженим доступом, чітко розмежувати поняття «конфіденційна та інша передбачена законом таємниця» і встановити правовий режим кожного виду такої інформації, який включатиме перелік відомостей, що можуть бути віднесені до відповідної категорії інформації з обмеженим доступом та гриф (грифи) обмеження такого доступу, компетенцію суб'єктів інформаційної діяльності у вирішенні цих питань. Крім того, вказаний закон має визначити механізм набуття і реалізації права власності громадян, юридичних осіб на інформацію (інформаційні ресурси), а також держави — на інформаційні ресурси з обмеженим доступом, створені повністю або частково за рахунок коштів державного бюджету.

" Закон України «Про захист інформації» має визначити державну систему захисту інформації з обмеженим доступом та відкритої інформації, важливої для особи, суспільства, держави; режим доступу до інформації з обмеженим доступом, починаючи від виготовлення інформаційної продукції і технологій; повноваження всіх суб'єктів інформаційної діяльності — від державних органів до громадян на предмет їхніх прав і обов'язків

щодо захисту інформації, а також загальні принципи і механізми захисту інформації (організаційні, правові, технічні, криптографічні).

До Закону України «Про захист інформації» можуть бути включені розділи щодо міжнародної діяльності у сфері захисту інформації з визначенням порядку взаємодії в цих питаннях з іншими країнами; про забезпечення інформаційних прав нашої держави в процесі міжнародного співробітництва; про регулювання захисту інформаційних ресурсів під час використання глобальних інформаційних систем типу Інтернет. Альтернативним варіантом може бути розроблення і прийняття Закону України «Про міжнародний інформаційний обмін» з чітким визначенням правових норм щодо регулювання відносин у перелічених напрямках інформаційної діяльності.

У законах «Про інформацію з обмеженим доступом» та «Про захист інформації» щодо видів інформації, відносини у сфері діяльності з якими регулюються окремими актами законодавства (наприклад, «державна таємниця»), доцільно зробити посилення на відповідні закони.

Відносини в інформаційній сфері регулюються відповідними актами законодавства, однак вони визначають лише основні принципи і вимоги до захисту інформаційних ресурсів з обмеженим доступом та відкритої інформації, важливої для особи, суспільства, держави. Принципи і вимоги актів законодавства реалізуються через систему підзаконних актів, що регламентують зміст роботи по забезпеченню захисту інформаційних ресурсів на всіх етапах їх формування, зберігання, поширення і розвитку. Систему науково обґрунтованих нормативно-правових актів, що стосується захисту інформації з обмеженим доступом та відповідної відкритої інформації (щодо державної таємниці та ТЗІ — розглядається в окремих розділах), ще належить створити.

В умовах бурхливого розвитку інформатизації, становлення інформаційного суспільства, перетворення інформації на стратегічний ресурс, а його формування і поширення на окрему галузь виробництва є актуальним наукове обґрунтування необхідності визначення правовою доктриною держави інформаційного права як окремої галузі юридичної науки з відповідним правовим і організаційним забезпеченням її функціонування. Тільки

в межах галузевої юридичної науки, на відповідно створеній науковій базі можна науково обґрунтувати предмет, систему інформаційного права, всі аспекти правового регулювання відносин в інформаційній сфері, структури організаційного забезпечення її функціонування та сформувати необхідний інтелектуально-кадровий потенціал для цієї сфери діяльності.

На думку автора, не можна ігнорувати гостроти і актуальності порушених у даній праці проблем: можна вести мову про єдиний економічний простір або вільний ринок країн СНД, можна навіть вступити до СОТ, однак неврегульованість у сфері інформаційних відносин незабаром виявить себе, як, до речі, вже виявляє себе як гальмівний фактор на шляху інноваційного розвитку всередині країни, стримуючи інформаційний обмін як між наукою і виробництвом, так і між суб'єктами господарювання.

Може виникнути запитання, а чи не надто багато уваги приділяється питанням захисту інформаційних ресурсів? Слушне запитання, хоча і не для фахівців.

Для того щоб відповісти на нього, треба усвідомити, що в Україні є ряд науково-технічних розробок і технологій, які не мають аналогів у світі. Це є важливою частиною інформаційно-інтелектуального потенціалу нації, забезпечуючи на даному етапі і в майбутньому її статус у світі як розвинутої в науково-технологічному відношенні держави, створюючи основу системи національної безпеки.

Ми живемо в конкурентному світі, а конкуренція інколи набуває вкрай жорстких форм, і про це потрібно прямо говорити. Треба, наприклад, уявити для себе, з чим ми зіткнемося, вступаючи до СОТ; як організаційно побудовані органи виконавчої влади країн, які в СОТ не є новачками, і які функції вони виконують; як забезпечується координація дій між державою та суб'єктами господарювання в таких країнах; як здійснюється інформаційне «підживлення» державою науки і промисловості в країнах з ринковою економікою та ін.

ВИСНОВКИ

У монографії здійснена спроба виробити єдиний підхід до проблеми державного управління національними інформаційними ресурсами з наукового потенціалу України, який дає можливість системного бачення проблеми, враховує організаційно-правові, структурні та функціональні особливості об'єкта управління, в тому числі визначає можливості інформаційного обігу за результатами науково-технічної діяльності згідно з вимогами національної безпеки держави в умовах політичної, економічної та соціальної трансформації суспільства.

Підхід, що пропонується, зважаючи на геополітичні закономірності та тенденції реформування суспільно-економічних систем, ґрунтується на засадах визначення інформаційної діяльності за вітчизняним науково-технічним доробком як складової державної науково-технологічної, інноваційної та регуляторної політики. При цьому процес формування та використання змістовного інформаційного ресурсу за таким доробком становить сутність інформаційної діяльності. На етапі входження України до європейської спільноти внутрішня інформаційна діяльність додатково зумовлюється глобальними економічними та політичними чинниками, що й веде до необхідності визначення адекватних організаційних, правових, методологічних засад розвитку такої діяльності на державному рівні.

Нова економічна і політична ситуація, яка виникла в Україні на етапі переходу до ринкових відносин, сучасні тенденції в демократизації суспільного розвитку внесли суттєві зміни у погляди на систему національних інформаційних ресурсів і соціально-економічні механізми її функціонування як на склад-

ну, порівняно автономну систему і водночас як на об'єкт державного управління.

У праці показано, що сама сутність інформаційного ресурсу за науковим потенціалом України передбачає міждисциплінарний підхід до еволюції його становлення, врахування як ретроспективного аналізу використання ресурсу, так і стратегічного, з метою опрацювання та обґрунтування відповідних стратегічних і практичних рішень.

Реалізація стратегії будь-якого типу значною мірою визначається організаційно-господарським механізмом, обраним для цієї мети. Показано, що організаційно-господарський механізм стратегії розвитку СНІР реалізується через сукупність елементів її організаційної та функціональної структури, форм управлінських відносин, методів та засобів, що діють у певний період та забезпечені певними правовими можливостями. Перехід до іншої стратегії передбачає зміну складу згаданих елементів, форм, методів та засобів, що свідчить про динамічність такого механізму, а власне зміни, їх легітимність закріплюються відповідними правовими можливостями.

Процесу трансформації інформаційної діяльності в Україні властиві слабке і непослідовне впровадження ринкових відносин і невідповідність до таких відносин інформаційної інфраструктури, що стримує позитивну адаптацію СНІР до умов конкуренції. Відверто слабкою постає інформаційна політика щодо цілеспрямованої підтримки формування потенціалу конкурентоспроможності галузей і виробництв, особливо наукоємних. Збереження ЗІР з науково-технічного та освітнього компонентів стає дедалі проблематичнішим як через недостатнє фінансування саме цих секторів діяльності, так і через відсутнє відставання у створенні сучасних організаційно-виробничих умов для відповідних інформаційних інфраструктур.

Найбільш яскраво прорахунки в напрямі ринкової спрямованості трансформації інформаційної діяльності, її безсистемність проявились в аспекті політики інформатизації, яка значною мірою підмінила собою державну інформаційну політику у сфері формування і використання національного інформаційно-змістовного ресурсу та керовану стратегію його розвитку.

До певної міри доводиться заново осмислювати наслідки інформатизації та вирішувати питання про напрям інтеграції

до світового інформаційного простору: поновлювати колишні канали з подальшою їх модифікацією або ж створювати сучасну систему, яка має бути з самого початку орієнтованою на відкритість та повну сумісність із світовими інформаційними потоками. Враховуючи, що економіка України все ще перебуває у процесі трансформації за всіма напрямками господарювання, можливість маніпулювання з боку третіх країн процесами реорганізації української економіки через вплив на інформаційні потоки (їх насиченість, доступність, предметну змістовність) можна вважати однією із форм інформаційної загрози. Змінити цю ситуацію можна лише шляхом комплексного цілеспрямованого впливу на процеси інформаційної діяльності в Україні, сприяючи розвитку інформаційної інфраструктури, на засадах регуляції якої з боку держави і можливе сучасне інтегрування України у світовий інформаційний простір.

За таких умов впровадження стратегічного управління СНІР логічно зумовлює вибір самої стратегії, організацію управління — вибір моделі розвитку виробничих механізмів реалізації стратегії.

Інституційний характер змістовного інформаційного ресурсу диктує відповідну логіку побудови системи. Змістовний інформаційний ресурс (ЗІР) і інформаційна інфраструктура держави утворюють основу побудови національного інформаційного простору.

Стратегію і тактику управління визначає закон (правове поле), який закріплює інституційний характер формування і використання інформаційного ресурсу й реалізується у вигляді організаційно-правових засад, організаційних, методичних та технологічних заходів управління національним інформаційним ресурсом.

Стратегія управління здійснюється на рівні прийняття політичних рішень, з урахуванням як базового — інституційного принципу побудови СНІР, так і процесів формування, розвитку, використання ЗІР, перетворення його на науковий, промисловий, грошовий капітал на засадах, обумовлених правовими та методологічними положеннями здійснення інформаційної діяльності, тобто тактики управління.

На стратегічному рівні визначаються національні інтереси та відповідні їм пріоритети в інформаційній сфері, формуються

правові засади побудови, розвитку системи та управління нею. На основі головної стратегічної мети державної інформаційної політики з використання результатів науково-технічної діяльності визначаються функції та їх раціональний розподіл між організаційними (виробничими) структурами, що створюються або реорганізуються для досягнення цих цілей; формуються основні види стратегічного забезпечення системи управління СНІР; здійснюється прогнозування розвитку інформаційної сфери та прийняття державних політико-правових рішень щодо удосконалення системи управління у цій сфері з урахуванням вимог національної безпеки України. Цей рівень поданий як модель системної трансформації, що впливає з принципів стратегії управління.

Проведення дослідження системної трансформації інформаційної Діяльності в процесі переходу від централізованої планової до ринкової економіки дає можливість зробити основні висновки, які мають наукове і практичне значення для формування і здійснення стратегії управління інформаційним ресурсом з наукового потенціалу України.

Перехід від централізованої планової до ринкової економіки вимагає системних, методологічно послідовних реорганізацій, які можуть забезпечувати досягнення стратегічного успіху і мають незворотний характер. Процес трансформації інформаційної діяльності має відбуватися на засадах здійснення послідовної державної політики відтворення результатів науково-технічної діяльності у змістовному інформаційному ресурсі в межах системи національних інформаційних ресурсів і бути органічно пов'язаним із внутрішньою економічною та науковою політикою, системою національної безпеки, включений до сфери міжнародної діяльності з інформаційного обігу. Значну роль у цьому має відігравати прискорене здійснення інституційних перетворень щодо СНІР, проведення організаційно-адміністративних заходів з метою формування системи державного регулювання інформаційної діяльності для комерційного використання науково-технічних здобутків у їх інформаційному вигляді.

Суттєвими чинниками побудови і розвитку СНІР є інтегральний потенціал організаційних структур, віднесених до складу інформаційної інфраструктури, діяльність якої зумовлена динамікою процесів формування та використання ЗІР. Це вимагає

цілеспрямованої оптимізації структури СНІР і розробки диверсифікованої стратегії щодо використання змістовного інформаційного ресурсу. Формування логічно завершеної системи управління національними інформаційними ресурсами доцільно здійснювати шляхом удосконалення існуючої системи. Визначення, правове і організаційне закріплення провідних напрямів державної політики щодо управління національними інформаційними ресурсами має впливати з об'єктивних законів розвитку інформаційної сфери та державної управлінської діяльності. Процес формування системи державного управління національними інформаційними ресурсами має забезпечити цілісність СНІР, системний підхід до її побудови, стабільність організації та відстежуваність її зв'язків у процесі здійснення інформаційної діяльності, а також врахування об'єктивних якостей і характеристик змістовних інформаційних ресурсів за результатами науково-технічної діяльності, засобів їх обробки і передавання.

Особливості системної експлуатації інформаційного ресурсу у процесі його формування та розвитку дають змогу максимально використовувати організуючу функцію самого ресурсу та забезпечувати узгодженість усіх елементів СНІР та ПФС. Централізовані інформаційні фонди, що створюються за рахунок держбюджету — коштами регіонів та відомств, у процесі інформаційної взаємодії з приватними становлять основу національного інформаційного простору, який є упорядкованим об'єктом функціонального державного управління.

Кожен із організаційних елементів такої інформаційної інфраструктури є суб'єктом поширення інтелектуального продукту і претендує на певну частину прибутків від його реалізації. Інформаційна діяльність, що відбувається на запропонованих засадах, дає можливість трансформувати науково-технічні досягнення в економічну форму розвитку продуктивної сили держави.

Необхідно розмежувати повноваження між центральними і місцевими органами виконавчої влади, органами місцевого самоврядування, що передбачає:

- упорядкування системи суб'єктів управління із закріпленням за ними розпорядчих і контрольно-наглядових функцій, що посилює управлінську вертикаль;

- законодавче впорядкування організаційно-правових засад формування і розвитку ЗІР у межах чинної інформаційної

інфраструктури, а також державної координації її розвитку шляхом оптимізації регулятивного впливу на комплексний розвиток виробничих засад, концентрації інформаційної діяльності на відповідних рівнях ПФС, стимулювання інвестиційної та інноваційної активності щодо інформаційних технологій, мобілізації зовнішніх джерел поповнення змістовних інформаційних ресурсів;

- розробку концепції розвитку системи національних інформаційних ресурсів за її складовими і стратегії управління на підставі принципів формування стратегій розвитку ПФС, змісту управління;

- удосконалення функціональних механізмів управління стосовно головних об'єктів системи національних інформаційних ресурсів — науково-технічної інформації, охорони об'єктів інтелектуальної власності, трансферу технологій шляхом визначення цієї функції в системі структур виконавчої влади, законодавчого закріплення реалізації функцій з питань проведення державної інформаційної політики;

- введення практики горизонтальної та вертикальної інтеграції, формування вертикальних та горизонтальних організаційних елементів інфраструктур, системи заходів з формування ринку ЗІР (а не тільки інформаційних технологій) та підвищення ефективності його використання, що є змістом державної функціональної інформаційної політики, адаптованої до державної та приватної форм здійснення інформаційної діяльності;

- забезпечення комерційного напрямку розвитку СНІР шляхом законодавчого закріплення інституту власності на різні види ЗІР, визначення статусу спільної власності на інформаційні об'єкти, використання інституту спільного фінансування, залучення альтернативних джерел фінансування на засадах кооперування з прибутковими видами діяльності.

У монографії визначено лише окремі аспекти такого спеціального питання, як економічна розвідка і тільки в контексті векторів її інтересів у сфері інформаційних ресурсів. У світі працює добре налагоджена система пошуку необхідної інформації, і захистити змістовні інформаційні ресурси можна лише застосуванням комплексу системних заходів з боку як державних спеціальних служб, так і суб'єктів економічної та інформаційної діяльності.

У сучасних умовах розмежування «відкритої» інформації, доступ до якої вільний, і «закритої», доступ до якої охороняється законом, має вирішальне значення. Однак це розмежування ускладнюється виникненням так званої проміжної інформації, яка перебуває в зоні юридичного вакууму і відокремлює відкриту інформацію від закритої, а також у нейтральній зоні, що лежить між відкритими пошуками змістовної інформації з використанням законних методів і таємних пошуків з використанням незаконних методів. Ця «проміжна зона» зростає як у зв'язку з труднощами контролю обсягів інформації, які повсякчас збільшуються, і складними юридичними ситуаціями, так і у зв'язку із запеклістю конкурентної боротьби.

В умовах конкурентної боротьби на міжнародному ринку масштаби «полювання» на «закриту» і «проміжну» інформацію різко зростають, що зумовлено спрямованістю суб'єкта на заощадження власних коштів на науково-дослідні та дослідно-конструкторські роботи (НДДКР), а також фундаментальні дослідження, бажанням бути в курсі справ конкурента, використовувати його науково-технічні досягнення у власних інтересах. Тому надзвичайно важливо, щоб будь-яка робота в державі з інформаційними ресурсами, що містять відомості обмеженого доступу, здійснювалася відповідно до «правил гри», встановлених державою для кожного виду інформаційних ресурсів, оскільки бурхливий розвиток інформаційних технологій, зміна методів пошуку інформації розширюють зону загроз змістовним інформаційним ресурсам, яка є загальною для оборонної і цивільної промисловості.

Саме тому у сфері економічної розвідки визначилися такі основні напрями професійного інтересу: науково-дослідні і конструкторські роботи; фінансові операції компаній, у тому числі фінансування проектів, інвестиційна політика; особливості технологічного процесу, специфікації продукції, результати випробувань; маркетинг і, зокрема, режим постачань, списки замовників, кон'юнктура ринку, відомості про угоди, що укладаються, а також звіти про реалізацію продукції; організація виробництва, у тому числі дані про вразливі місця діючих і передбачуваних партнерів і конкурентів; постійна спрямованість на пошук науково-технічної інформації «випереджання» — значні науково-технічні досягнення, прориви у фундаментальних дос-

лідженнях та іншій пріоритетній проблематиці; прагнення до одержання кризової індикаторної інформації, насамперед щодо об'єктів валютно-фінансової сфери і паливно-енергетичного комплексу.

За цих умов особливого значення набуває випереджаюче вдосконалення і розвиток правової, організаційної, організаційно-технічної і ресурсної бази системи захисту інформаційних ресурсів України, передусім вітчизняного науково-технічного доробку.

Враховуючи, що інформаційна безпека Конституцією України віднесена до найважливішої функції держави, а складовою інформаційної безпеки є безпека сфери створення і використання інформаційних ресурсів (СНІР), було б доцільним на рівні законів чітко визначити правові засади реалізації державної інформаційної політики щодо захисту цих ресурсів:

- на вищому державному рівні на основі політичних рішень, законодавчих, нормативно-правових актів сформувати правові засади єдиної державної інформаційної політики щодо формування, поширення, використання й захисту ЗІР;

- на організаційному рівні державної виконавчої влади розробити і впровадити міжгалузеву, відомчу нормативно-методичну базу, технологічні аспекти щодо оперативного управління формуванням, поширенням, використанням і захистом змістовних інформаційних ресурсів з урахуванням форми їх існування в єдиній системі національних інформаційних ресурсів;

- на виконавчому рівні в апаратах державних органів, на підприємствах, в установах і організаціях забезпечити комплекс заходів для безпосереднього виконання законодавчих і нормативно-правових актів, вимог нормативно-методичних документів, порядку і правил, встановлених органами виконавчої влади щодо формування, поширення, використання й захисту інформаційних ресурсів, розробити внутрішні нормативно-методичні документи (положення, інструкції, методики) для керівництва в практичній роботі структурних підрозділів та посадових осіб.

На виконавчому рівні — в межах інформаційної інфраструктури — безпосередньо реалізується комплексна система формування, поширення, використання й захисту інформаційних ресурсів за науковим потенціалом України. Від сталого функціо-

нування цієї системи залежатиме функціонування як відомчих, міжвідомчих, так і загальнодержавних засад управління СНІР та її захист.

Впровадження в практику управління інформаційно-аналітичною діяльністю основних положень монографії та рекомендацій щодо сфери системних досліджень й організації управління підтвердило достовірність результатів, отриманих у процесі дослідження.

ПРИМІТКИ

¹ *Энциклопедия I* Редкол.: И. Е. Баренбаум, А. А. Беловицкая, А. А. Говоров и др. — М.: Большая Российская энциклопедия, 1998. — 800 с.

² *Peter Large. The Micro Revolution Revisited.* New Jersey: Rowman and Allanheld Company, 1984.

³ *Информационная безопасность России* / Ю. С. Уфимцев, Е. А. Ерофеев и др. — М.: Изд-во «Экзамен», 2003. — 560 с.

⁴ *США на рубеже веков* / Редкол.: С. М. Рогов, В. А. Федорович, В. А. Кременюк и др. — М.: Наука, 2000. — С. 139.

⁵ *Там само.* — С. 147.

⁶ *Там само.* — С. 145.

⁷ *Там само.* — С. 141.

⁸ *Там само.* — С. 140.

⁹ *Информационная безопасность России* / Ю. С. Уфимцев, Е. А. Ерофеев и др. — М.: Изд-во «Экзамен», 2003. — 560 с.

¹⁰ *Там само.*

¹¹ Юсупов Р. М., Заболотский В. П. Научно-методологические основы информатизации. — СПб.: Наука, 2000. — С.5.

¹² Макаренко Е. А. Інформаційне суспільство, політика, право в програмній діяльності ЮНЕСКО. — • К.: Науково-вид. центр «Наша культура і наука», 2002. — С.29—51.

¹³ Юсупов Р. М., Заболотский В. П. Научно-методологические основы информации. — С.11.

¹⁴ Макаренко Е. А. Інформаційне суспільство, політика, право в програмній діяльності ЮНЕСКО. — С.36.

¹⁵ Юсупов Р. М., Заболотский В. П. Научно-методологические основы информатизации. — С.11.

¹⁶ Макаренко Е. А. Інформаційне суспільство, політика, право в програмній діяльності ЮНЕСКО.

- ¹⁷ Юсупов Р.М., Заболотский В.П. Научно-методологические основы информатизации. — С.11 — 13.
- ¹⁸ Там само. — С.17—22.
- ¹⁸ Древнегреческая философия. От Платона до Аристотеля: Соч. / Пер. с древнегреч. — Х.: Фолио, М.: ООО «Фирма «Изд-во АСТ», 1999. — С.441.
- ²⁰ Юсупов Р.М., Заболотский В.П. Научно-методологические основы информатизации. — С.42.
- ²¹ Там само. — С. 5.
- ²² Халипов В. Ф. Кратология как система наук о власти. — М.: Республика, 1999. — С.23.
- ²³ Тироф Р. Обработка данных в управлении: В 2 т. — М.: Мир, 1976. — Т.2. — С. 484.
- ²⁴ Соснин О. В. Концепт інформаційної політики у сучасному світі // Гуманітарний журнал Національної гірничої академії України (м. Дніпропетровськ). — 2001. — №3—4 (11—12). — С.155 — 166.
- ²⁶ Закон України «Про пріоритетні напрями інноваційної діяльності в Україні» // Урядовий кур'єр. — 2003. — 19 лют.
- ²⁶ Терещенко В. И. Проблема выбора: Политика научных приоритетов на Западе. — К.: Политиздат Украины, 1989. — С. 3 — 7.
- ²⁷ Там само. — С. 9.
- ²⁸ Утвердження інноваційної моделі розвитку економіки України: Матеріали наук.-практ. конф. — К.: НТУУ «КПІ», 2003. — 434 с
- ²⁹ Глушков В., Доброе Г., Терещенко В.И. Беседы об управлении. — К.: Политиздат Украины, 1973. — С.67.
- ³⁰ Там само. — С. 68.
- ³¹ Там само. — С. 69.
- ³² Андрейчиков А.В., Андрейчикова О.Н. Анализ, синтез, планирование решений в экономике. — М.: Финансы и статистика, 2001. — С.9 — 11.
- ³³ Анфилов В.С. и др. Системный анализ в управлении: Учеб. пос. / В.С. Анфилов, А.А. Емельянов, А.А. Кукушкин; Под ред. А.А. Емельянова. — М.: Финансы и статистика, 2002. — С.3 — 5.
- ³⁴ Лестер К. Туроу Будущее капитализма. Как сегодняшние экономические силы формируют завтрашний мир / Пер. с англ. А. И. Федорова. — Новосибирск: Сибирский хронограф, 1999. — С. 58 — 59.
- ³⁵ Власенко О.С. Книга памяти «Арсенал» 1945—90 гг. — К.: КВШ, 2003. — 336 с.
- ³⁶ Бесчасный Л.К., Соснин А.В., Иванов В.В. и др. Принципы построения системы экономических взаимоотношений научных учреждений и организаций АН УССР с предприятиями отрасли. — К., 1991. — 48 с. (Препринт АН УССР. Ин-т экономики АН УССР. 91—1).

- ⁸⁷ Бандурин В.В. Участие ФГУП «Рособоронэкспорт» в реализации государственной инновационной политики // Инновация. — 2001. — №7 (44). — С. 30 — 32.
- ⁸⁸ Власенко О.С. Книга памяти «Арсенал» 1945—90 гг. — С.263.
- ³⁹ Гриняев С.Г. Война в четвертой сфере. Превосходство в киберпространстве будет определять победу в конфликтах XXI века // Независимое военное обозрение. — 2000. — №42.
- ⁴⁰ Горбачев Ю., Тюрин В. К вопросу о «войне в четвертой сфере» // Независимое военное обозрение. — 2000. — №42.
- ⁴¹ Мастяница Й.У., Соснин О.В., Шиманский Л.Е. Інформаційні ресурси України: проблеми державного управління. — К.: НІСД, 2002. — С 35, 51.
- ⁴² Соловьев В. Военные реформы в Европе: проблемы, удачи и неудачи // Независимое военное обозрение. — 2001. — № 14.
- ⁴⁸ Жуков В. Взгляды военного руководства США на ведение информационно-войны // Зарубежное военное обозрение. — 2001. — №1. — С.2.
- ⁴⁴ Дежин Е. Атака на разум противника. Китайские психологические операции в свете национальных традиций // Независимое военное обозрение. — 2001. — №1(223).
- ⁴⁵ Перечень основных направлений фундаментальных исследований в области оборонной безопасности (Академия военных наук формулирует темы приоритетных научных разработок) // Независимое военное обозрение. — 1999. — №5. — С.4.
- ⁴⁶ Сокут С. Общественная организация решает государственные проблемы (Академия военных наук обсудила пути вывода российских силовых структур из кризиса) // Независимое военное обозрение. — 1999. — №7. — С.3.
- ⁴⁷ Андреев В. Новые тенденции развития средств противоборства // Независимое военное обозрение. — 1999. — №7. — С.6.
- ⁴³ Философский словарь / Под ред. М.М. Розенталя и П.Ф. Юдина. — М., 1963. — С.172.
- ⁴⁹ Там само. — С. 524.
- ⁵⁰ Там само. — С. 173.
- ⁵¹ Там само.
- ⁵² Там само. — С. 161.
- ⁵³ Глушков В., Доброе Г., Терещенко В. Бесіди про управління. — К.: Політвидав України, 1973. — С.15.
- ⁵⁴ Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство/ Санкт-Петербургский университет МВД России. — СПб.: Фонд «Университет», 2000. — С.27.
- ⁵⁵ Закон України «Про інформацію» від 2 жовтня 1992 р. — К., 1992. — Ст.650, 651.

⁵⁶ *Информационные ресурсы России: Спр. (колл. авт. под общей ред. Реймана Л.Д.)* — М.: ФИОРД-ИНФО, 2000. — С. 12.

⁵⁷ *Закон України «Про інформацію»* від 2 жовтня 1992 р. // *Закони України*. — К: Книга, 1996. — Т.4. — С.72–88.

⁵⁸ *Яро науково-технічну інформацію: Закон України* від 25 червня 1993 р. // *Закони України*. — К.: Книга, 1996. — Т.5. — С.191–200.

⁵⁹ *Соснін О.* Інформаційний суверенітет України: правові аспекти встановлення режиму доступу до інформаційних ресурсів України // *БОРИСТЕН*. — 2002. — №5. — С. 13 — 15.

⁶⁰ *Толковый словарь по основам информационной деятельности* / Под. ред. д.э.л. Ермошенко Н.Н. — К.: УкрАИН-УкрИНТЭИ, 1995. — С.248.

⁶¹ *Лаврухин А.Н.* «Информационное общество»: надежды и результаты информатизации // *Сб. трудов ВНИИСИ*. — М., 1989. — Вып. 12. — С. 43.

⁶² *Белл Д.* Социальные рамки информационного общества // *Новая технократическая волна на Западе*. — М.: Прогресс, 1986. — С. 394; *Ракитов А.И.* Наш путь к информационному обществу // *Теория и практика общественно-научной информации*. — М.: ИНИОН, 1989; *Курное И.Н.* Информационное общество и Россия: особый путь // *Инф'орм-ревю*. — 1997. — №4(24). — С. 4—5; *Learning in the Information society. Action Plan for European education initiative (1996–1998)*; *Урсул А.Д., Урсул Т.А.* На пути к устойчивому развитию цивилизации: информационные факторы // *Информационное общество*. — 1997. — № 2—3. — С. 20—27; *Макаренко Є.А.* Идеология информационного общества та правові проблеми інформаційного поля // *Актуальні проблеми міжнародних відносин*. — К., 1999. — Вип.14. — 4.1; *Макаренко Є.А.* Інформаційне суспільство, політика, право в програмній діяльності ЮНЕСКО. — К.: Наша культура і наука, 2002; *Макаренко Є.А.* Європейська інформаційна політика: Моногр. — К.: Наша культура і наука, 2000. — 368 с

⁶³ *Шеннон Р.* Имитационное моделирование систем: искусство и наука. — М.: Мир, 1978. — С. 15.

⁶⁴ *Юсупов Р.М., Заболотский В.П.* Научно-методологические основы информатизации. — С.29.

⁶⁵ Цит. за: *Там само*. — С. 293.

⁶⁶ *Кляхин Д.* Сотрудники Национальной академии наук выдвинули экономические требования // *Сегодня*. — 2003. — 19 июня. — С.5.

⁶⁷ *Методология и стратегические цели развития России* // *Национальная безопасность и геополитика России*. — 2002. — №10–11. — С.183.

⁶⁸ *Систематизація законодавства України: проблеми та перспективи вдосконалення: Моногр.* — К.: Ін-т держави і права ім. Корещука НАН України, 2003. — С.160.

⁸⁰ *Юсупов Р.М., Заболотский В.П.* Научно-методологические основы информатизации. — С.294.

⁷⁰ *Макаренко Є.А.* Європейська інформаційна політика: Моногр.; *Горина С.А., Козьменко С.Н.* Банковская система и экономика: реструктуризация на фоне глобализации. — М.: МАКС Пресс, 2001. — 324 с.

⁷¹ *Толочко П.* Неисповедимы пути Украины // *Зеркало недели*. — 2001. — 20 окт. — С.17.

⁷² *Закон України «Про національну програму інформатизації»* від 4 лютого 1998 р. — К., 1998.

⁷³ *Закон України «Про інформацію»* від 2 жовтня 1992 р. — К., 1992.

⁷⁴ *Закон України «Про науково-технічну інформацію»*.

⁷⁵ *Проект Закону України «Про інформаційний суверенітет та інформаційну безпеку України»*. Внесено на розгляд Верховної Ради України.

⁷⁶ *Актуальні проблеми інформаційної безпеки України. Аналіт. доп. УЦЕПД* // *Національна безпека і оборона*. — К, 2001. — №1. — С.2—59.

⁷⁷ *Бондаренко В.О., Литвиненко О.В.* Глобальна ідейно-політична гегемонія та становлення нових незалежних держав // *Стратегічна панорама*. — К, 2000. — №3—4. — С.156—160; *Дешко А.І., Слівак А.Є.* Проблеми організації єдиного інформаційного простору України // *Науково-технічна інформація*. — К, 2000.—№3. — С.14—18; *Лазарев Г.* Захист інформації в інформаційно-телекомунікаційних системах // *Національна безпека і оборона*. — К., 2001. — №1. — С.80 — 83; *Національна безпека України 1994–1996 рр.: Наук. доповіді НІСД / Редкол.: Белов О. Ф. (голова) та ін. — (Сер. «Загальноінститутські доповіді»)*. — К.: НІСД, 1997. — 200 с; *Концепція (Основи державної політики) національної безпеки України*. Схвалено Постановою Верховної Ради України від 16 січня 1997 р. — К, 1997.

⁷⁸ *Закон України «Про інформацію»*. — Ст.28, 30.

⁷⁹ *Закон України «Про державну таємницю»* в ред. від 21 вересня 1999 р. // *Голос України*. — 1999. — 26 жовт.

⁸⁰ *Там само*. — Ст.6.

⁸¹ *Закон України «Про інформацію»*. — Ст. 5, 28, 30, 45, 47, 53, 54.

⁸² *Закон України «Про науково-технічну інформацію»*. — Ст.1.

⁸³ *Там само*. — Ст. 14 — 15.

⁸⁴ *Там само*. — Ст. 15.

⁸⁵ *Конституція України* // *Закони України*. — К.: Книга, 1997. — Т.Ю. — С. 5—40. — Ст.34.

⁸⁶ *Закон України «Про інформацію»*. — Ст. 28.

⁸⁷ *Закон України «Про державну таємницю»*. — Ст. 1.

⁸⁸ *Там само*. — Ст.9, 10, 11.

- ⁸⁹ Там само. — Ст.И.
- ⁹⁰ Там само. — Ст.9.
- ⁸¹ Там само. — Ст.Ю.
- ⁹² Там само. — Ст.12.
- ⁹³ Секретная информация в сфере национальной безопасности: Директива Президента США от 17.04.95, № 12958 // Сб. норм. док. № 19. — К: Держкомсекретів України, 1999. — С.2-27. — Розд. 1.5.
- ⁹⁴ Там само. — Розд. 1.4.
- ⁹⁶ Там само. — Розд. 2.1, 2.2.
- ⁹⁶ Закон Российской Федерации «О государственной тайне» от 6 октября 1997 г. // Российская газета. — 1997. — 9 окт. — Ст.5.
- ⁹⁷ Там само. — Ст.9.
- ⁹⁸ Закон. України «Про державну таємницю». — Ст. 8.
- ⁹⁹ Там само. — Ст.15.
- ¹⁰⁰ Секретна інформація в сфері національної безпеки. Директива Президента США від квітня 1995 р., №12958 // 36. №19. — К.: Держкомсекретів України, 1999. — С.2 — 27. — Розд. 1.3.
- ¹⁰¹ Закон Российской Федерации «О государственной тайне» от 21 июля 1993. — Додаток №3 до: Ярочкин В.И. Информационная безопасность: Учебн. пособ. — М.: Междунар. отношения, 2000. — С.279-301. — Ст.8.
- ¹⁰² Шиверский А.А. Защита информации: проблемы теории и практики. — М.: Юрист, 1996. — С.19.
- ¹⁰³ Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності. Затверджено наказом Держкомсекретів України від 9 лютого 1998 р. №23. 36. №8. — К.: Держкомсекретів України, 1998. — С.4 — 24.
- ¹⁰⁴ Там само. — Розд.2.
- ¹⁰⁵ Про порядок оформлення і використання прав на винаходи, корисні моделі і промислові зразки: Положення, затверджене Постановою Верховної Ради України від 19 січня 1995 р. // Голос України. — 1995. — 14 лют. — П. 4.
- ¹⁰⁶ Там само. — П.7.
- ¹⁰⁷ Там само.
- ¹⁰⁸ Там само. — П.3.
- ¹⁰⁹ Закон України «Про державну таємницю». — Ст. 13.
- ¹¹⁰ Там само. — Ст.14.
- ¹¹¹ Там само. — Ст.12.
- ¹¹² Звід відомостей, що становлять державну таємницю. Затверджено наказом СБ України від 01.03.2001, № 52. — Чинний з 13 квітня 2001 р.
- ¹¹³ Закон України «Про державну таємницю». — Ст. 1.
- ¹¹⁴ Там само.
- ¹¹⁵ Там само. — Ст.15.
- ¹¹⁶ ТОЛІ СОЛЮ. — Ст.39.
- ¹¹⁷ Там само. — Ст.16.
- ¹¹⁸ Положення про порядок оформлення і використання прав на винаходи, корисні моделі і промислові зразки, що становлять державну таємницю. Затверджено Постановою Верховної Ради України від 19 січня 1995 р. // Голос України. — 1995. — 14 лют.
- ¹¹⁹ Талг салю. — Пункти 4 — 5.
- ¹²⁰ Закон України «Про державну таємницю». — Ст. 19.
- ¹²¹ Там само. — Ст.3.
- иг Чубукова О.Ю. Державні та недержавні структури в процесі інформатизації суспільства / Експрес-новини: наука, техніка, виробництво. — К.: УкрШТЕІ, 1999. — Вип. 7—8. — С 34—35; Чубукова О.Ю. Організаційні засади формування інформаційної економіки // Проблеми науки. — 2002. — №4. — С.7—14.; Мастяниця Й.У., Саснін О.В., Шиманський Л. Є. Інформаційні ресурси України: проблеми державного управління / За заг. ред. О. В. Сосніна. — К.: НІСД, 2002. — 141 с; Концепція інноваційного розвитку України (проект) // Наука і наукознавство. — 2002. — Вип. 1 (35). — С.3 — 22.
- ¹²³ Marchard D.A., Horton F.W., jr. Infotrends: Profiting from your inform. Resources. — N.Y., Wiley, 1986. — XL — 324 p.; Араное М.В. Информатизация общества: зарубежный опыт // Вестник Академии наук СССР. — 1986. — № 9. — С. 62 — 77.
- ¹²⁴ Басова Т.Е. На рынке информационных услуг капиталистических стран // БИКЦ. — ВНИКИ. — 1984. — № 103. — С. 2.
- ¹²⁵ Сумароков Л.Н. Государственная информационная система по науке и технике, проблемы развития // Проблемы информационных систем. — 1987. — № 2. — С. 3 — 11.
- ¹²⁶ Kozłowski Ian. Zmiany w funkcjonowaniu N+T / Polit.nauk.kraj. gosp. rozwiniet.: Greneza, evol., probl. — Warszawa, 1992. — S. 19-23.
- ¹²⁷ Решения ЮНЕСКО 1996—1997 гг. // <http://www.unesco.org/publishing>; РЖ ВИНТИ Информатика, 1994. — №3—6. — Реф.37—40. — Библ. — 125 наим.
- ¹²⁸ Закон Российской Федерации «О статусе наукограда Российской Федерации» от 7 апреля 1999 года №70-ФЗ.
- ¹²⁹ Соснін О.В. Про критичні загрози національній безпеці України в науково-технологічній сфері, шляхи їх упередження або нейтралізації: Аналіт. матеріали НІСД. — К.: НІСД, 2001. — 37 с
- ¹³⁰ Талі салю.
- ¹³¹ Інтелектуальна власність в Україні: правові засади та практика / Наук.-практ. вид.: У 4 т. / За заг. ред. О. Д. Святоцького. — К: Ін Юре, 1999.

¹³² Хрустальова В. Сучасні проблеми вартісної оцінки об'єктів інтелектуальної власності // Експрес-новини: наука, техніка, виробництво. — 1997. — №23—24. — С.8-10; Хрустальова В. Інтелектуальні інвестиції в економіку України // Фінанси України. — 1998. — №8. — С 77 — 82.

¹³³ Подопригора А. А. Основы римского гражданского права: Учебн., 2-е изд. — К.: Вентури, 1994. — 288 с.

¹³⁴ Там само.

¹³⁵ Соснін О.В. Щодо проекту Концепції державної інформаційної політики України: Аналіт. матеріали НІСД. — К.: НІСД, 2000. — 23 с — Машинопис.

¹³⁶ Паляниця А. Регуляторна реформа в Україні: напередодні нового стану // Перспективні дослідження. — К., 1999. — №6. — С.4 — 16.

¹³⁷ Концепція державної регуляторної політики / Авт. кол.: В.Загородній (кер.), Г.Вілоус, М.Вареник та ін. // Перспективні дослідження. — К., 1999. — С.17 — 27.

¹³⁸ Андрушук Г. Інноваційна діяльність в Україні: економічний механізм стимулювання // ІВ. — 2000. — №12. — С.23 — 30.

¹³⁹ Закон України «Про основи державної політики України у сфері науки і науково-технічної діяльності» від 19 грудня 1991 р.

¹⁴⁰ Актуальні питання методології та практики науково-технологічної політики / За ред. Б. А. Малицького. Центр досл. науково-техн. потенціалу та історії науки ім. Г. М. Доброва НАНУ. — К.: УкрІНТЕІ. — 2001. — 204 с

¹⁴¹ Там само.

¹⁴² Закон України «Про спеціальний режим інвестиційної та інноваційної діяльності технологічних парків «Напівпровідникові технології і матеріали, оптоелектроніка та сенсорна техніка», «Інститут електрозварювання імені Є.О.Патона», «Інститут монокристалів» // Відомості Верховної Ради України. — 1999. — №40. — С.363.

¹⁴³ Актуальні питання методології та практики науково-технологічної політики / За ред. В. А. Малицького. Центр досл. науково-техн. потенціалу та історії науки ім. Г. М. Доброва НАНУ. — Розд. 1.4.

¹⁴⁴ Закон України «Про охорону прав на винаходи і корисні моделі» від 15 грудня 1993 р. // Закони України / Верховна Рада України; Ін-т законодавства. — К.: Книга, 1996. — Т.6.

¹⁴⁵ Актуальні питання методології та практики науково-технологічної політики / За ред. Б. А. Малицького. Центр досл. науково-техн. потенціалу та історії науки ім. Г. М. Доброва НАНУ. — 204 с

¹⁴⁸ Закон України «Про внесення змін і доповнень до Закону України «Про охорону прав на винаходи і корисні моделі» // Відомості Верховної Ради України. — 2000. — №37.

¹⁴⁷ Про заходи щодо охорони інтелектуальної власності в Україні: Указ Президента України від 27.04.01 №285 // Офіційний вісник України. — 2001. — №18. — 4.2. — С.820—821.

¹⁴⁸ Програма розвитку державної системи державної системи охорони інтелектуальної власності в Україні на 2001—2004 роки. Проект // ІВ. — 2000. — №12. — С.37—43.

¹⁴⁹ Штайльман К. Новая философия бизнеса: В 3 т. // Риски и успех предпринимательства в постсоциалистическом обществе. — Москва-Берлин: Рос. психол. общ-во. — 1998. — С.63—67.

¹⁵⁰ Цибульов П. Динаміка винахідницької діяльності в Україні // Матеріали V Міжнародної наук.-практ. конф.: Актуальні питання розвитку інноваційної діяльності та охорони інтелектуальної власності. — Алушта, 11—16 вересня, 2000 р.

¹⁵¹ Хрустальова В. Інтелектуальні інвестиції в економіку України // Фінанси України. — 1998. — №8. — С 77 — 82.

¹⁵² Рижих В.М. Государственное управление научно-техническим прогрессом: экономические аспекты. — Х.: Прапор, 1998. — 390 с.

¹⁵³ Там само. — С.316.

¹⁵⁴ Закон України «Про науково-технічну інформацію» від 25 червня 1993 // Закони України / Верховна Рада України; Ін-т законодавства. — К.: Книга, 1996. — Т.6. - С.191—200.

¹⁵⁵ Про підсумки роботи Міністерства освіти і науки в сфері наукової, науково-технічної діяльності за 2000 рік.: Доп. на засіданні Колегії МОН України, Київ, 27.03.2001 р. — К.: МОН України, 2001. — Машинопис.

¹⁵⁶ Там само. — С.27.

¹⁵⁷ Актуальні питання методології та практики науково-технологічної політики / За ред. Б. А. Малицького. Центр досл. науково-техн. потенціалу та історії науки ім. Г. М. Доброва НАНУ. — Розд.1.1.

¹⁵⁸ Про державну реєстрацію та облік НДДКР та дисертацій закритої тематики: Постанова Кабінету Міністрів України від 10.03.94 р. №155. — Чинна з 10 березня 1994 р.; Про державну реєстрацію НДДКР та дисертацій відкритої тематики: Постанова Кабінету Міністрів України від 31.03.92 р. №162. — Чинна з 31 березня 1992 р.

¹⁵⁹ Про систему науково-технічних програм: Постанова Кабінету Міністрів України від 03.06.93 №412 // Збірник законодавчих та нормативних актів України в сфері науки і науково-технічної діяльності. — Державна комісія з питань реорганізації в галузі науки. — К., 1996. — С 30.

¹⁶⁰ Актуальні питання методології та практики науково-технологічної політики / За ред. Б. А. Малицького. Центр досл. науково-техн. потенціалу та історії науки ім. Г. М. Доброва НАНУ. — С.75—76.

¹⁶¹ 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: Указ Президента України від 21.07.97 №663; Про рішення Ради національної безпеки і оборони України від 19 вересня 1997 року «Про стан науково-технічної сфери України та невідкладні заходи щодо підвищення ефективності її державного регулювання: Указ Президента України від 13.10.97 р. №1147; Про рішення Ради національної безпеки і оборони України від 3 липня 2001 року «Про невідкладні заходи щодо виводу з кризового стану науково-технічної сфери України і створення реальних умов для переходу економіки на інноваційну модель розвитку: Указ Президента України від 20.08.2001 №640; Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України: Указ Президента України від 06.12.2001 №1193.

¹⁶² Положение о государственной службе научно-технической информации: Постановление Правительства Российской Федерации от 25.07.97 г. №950//НТИ. — 1997. — №11. — С.24—26.

¹⁶³ О федеральной программе развития экспорта Российской Федерации: Постановление Правительства Российской Федерации от 08.02.96. №123.

¹⁶⁴ О государственной политике по вовлечению в хозяйственный оборот результатов научно-технической деятельности и объектов интеллектуальной собственности в сфере науки и технологий: Указ Президента Российской Федерации от 22.07.98 №863 // Собр. Законодат. РФ. — 1998. — №30. — Ст.3756; Об использовании результатов научно-технической деятельности: Постановление Правительства Российской Федерации от 02.09.99 №982.

¹⁶⁵ Мітрахович М. Охорона об'єктів промислової власності військового призначення // ІВ. — 2000. — №9—10. — С.56—59; Наказ Державного патентного відомства України «Про затвердження порядку видачі посвідчень України на винаходи, що становлять державну таємницю і охороняються авторськими свідоцтвами СРСР на секретні винаходи» від 23.01.96 №10. Зареєстровано в Міністерстві юстиції України 16.02.96 за №77/1102.

¹⁶⁶ Богорош. А., Денисюк В.А. К моделированию государственной инновационной политики // Бизнес-информ. — 1999. — №17—18; Гриньов Б.В., Денисюк В.А., Соловйов В.П. Деякі аспекти державного регулювання передачі (трансферу) технологій в Україні // Наука та наукознавство. — 1998. — №2. — С.3—12; Денисюк В. Про розвиток

системи передачі (трансферу) технологій в Україні для підвищення ефективності економіки // Наука та наукознавство. — 1999. — №14. — С.65—74; Чумаченко Б., Лавров К. Международный трансфер технологий: опыт американских корпораций // Проблемы теории и практики управления. — 1999. — №2. — С.3—14; Андрощук Г., Денисюк В.А. Государственное регулирование передачи технологий в США // Бизнес-информ. — 1997. — №22, 23.

¹⁶⁷ Долгое С.И. Глобализация экономики: новое слово или новое явление? — М.: Экономика, 1998. — С.215; Бжезинский З. Великая шахматная доска: Господство Америки и его геостратегические императивы. — М.: Междунар. отношения, 1999. — 254 с.

¹⁶⁸ Про реєстрацію алгоритмів і програм: Постанова Кабінету Міністрів України від 18.07.95 №532.

¹⁶⁹ Ларкин С. Что мы теряем из-за неумения использовать передовые технологии // Киевские новости. — 2000. — 17 фев.

¹⁷⁰ Копылов В. А. Информационное право. — М.: Юристъ, 1997. — 469 с.; Серпилина О., Хименко О. Организационно-правовые аспекты использования информационного ресурса государства // Информационные ресурсы НТИ: проблемы создания и использования: Материалы VIII Междунар. научно-практ. конф., Киев, 30—31 мая 2001 г. — К.: УкрИНТЕИ. — С. 114—117; Тихомиров Ю. А. Публичное право. — М.: Бек, 1995. — 485 с; Агапов А.Б. Основы государственного управления в сфере информатизации в Российской Федерации. — М.: Юристъ, 1997. — 343 с; Копылов В.А. Об основных теоретических положениях информационного права // НТИ. — 1998. — №8. — С.1—8; Дозорцев В.А. Система правового регулирования товарных информационных отношений // НТИ. — 1997. — №9. — С.2; Копылов В.А. К вопросу об информационной собственности // НТИ. — 1998. — №3. — С.3—5; Батурич Ю.М. Проблемы компьютерного права. — М.: Юрид. лит., 1991. — 271 с.

¹⁷¹ Авдошкин Е.Ф. Международные экономические отношения. — М.: Юристъ, 2001. — 366 с; Пгдопригора О. Правовая культура в законодательстве Украины про інтелектуальну власність // ІВ. — 2000. — №8—9. — С.6—12; Комерциализация интеллектуальной собственности: проблемы и решения / Сост. и общ. ред. Н. М. Фонштейн и В. Г. Зиновьева. — М.: Зел. О., 1996. — С.58—71.

¹⁷² Копылов В. А. Информационное право; Дозорцев В.А. Система правового регулирования товарных информационных отношений // НТИ. — 1997. — №9. — С.2; Батурич Ю. М. Проблемы компьютерного права.

¹⁷³ Воротшиїн Е.А. Антология права в теории институализма // Правоведение. — 1990. — №5. — С.43—46.

¹⁷⁴ Малащенко В.Ф. Конституція — Основний Закон держави // Погорілко В. Ф., Фрицький О. Ф., Городецький О. В. та ін. Конституційне право України: Підручн.; 2 вид. — К., 2000. — С.110.

¹⁷⁵ Мастяниця Й.У., Соснін О.В., Шиманський Л.Є. Інформаційні ресурси України: проблеми державного управління / За заг. ред. О. В. Сосніна.

¹⁷⁶ Гиляревский Р.С., Запаев Г.З., Родионов И.И., Цветкова В.А. Современная информатика. — М.: ВИНТИ, 1996. — С16.

¹⁷⁷ Підпригора О. Правова культура в законодавстві України про інтелектуальну власність // ІВ. — 2000. — №8—9. — С.6—12; *Коммерциализация интеллектуальной собственности: проблемы и решения* / Сост. и общ. ред. Н.М. Фонштейн и В.Г. Зиновьева. — С.58—71; Шербинин Ю.А. и др. Международные экономические отношения. Интеграция. — М.: ЮНИТИ, 1998. — 126 с.

¹⁷⁸ Маттеи У., Суханов Б.А. Основные положения права собственности. — М., 1999. — С.298; Харитонов Е.О., Саниахметова Н.А. Гражданское право: Частное право: Учебн. пос. — К., 2001. — С.224.

¹⁷⁹ Дзера О.В., Кузнецова Н.С., Підпригора О.А. та ін. Право власності в Україні: Навч. пос. / За заг. ред. О.В.Дзери, Н.С.Кузнецової. — К., 1996. — С.173; Музика Л. Власність в економічному та правовому вимірі // Право України. — 2001. — №12. — С.47—51.

¹⁸⁰ Там само.

¹⁸¹ Там само.

¹⁸² Шкредов В.П. Экономика и право: опыт экономико-юридического исследования общественного производства. — М.: Экономика, — 1990. — 269 с; Кучерявенко П.Х., Максименко Я.М. Разгосударствление собственности в переходной экономике Украины. — Х.: Консум, 1997. — 126 с; Крижанівський О. Обов'язок держави — захистити ефективного власника прав на ОІВ. // ІВ. — 2001. — №11. — С.49—55; Підпригора О. Правова культура в законодавстві України про інтелектуальну власність // ІВ. — 2000. — №8—9. — С.6—12.

¹⁸³ Там само.

¹⁸⁴ Там само.

¹⁸⁵ Там само.

¹⁸⁶ Закон України «Про науково-технічну інформацію». — Ст.2, абз.2.

¹⁸⁷ Дяків Т., Чуєв М. Оцінка нематеріальних активів — чий це клопіт? // ІВ. — 2001. — №3. — С.16—18; Рибалкін В.О., Лазня І.В. Теорія власності. — К.: Логос, 2000. — С.52.

¹⁸⁸ Проект Інформаційного кодексу України. Перша ред. проекту (на стадії узгодження). — К.: Держкомінформполітики, телебачення і радіомовлення України, 2001 р. — Машинопис.

¹⁸⁹ Информационные ресурсы России: Национальный доклад / Гл. ред. А.Е.Крупнов. — М.: Госкомсвязи России, 1999.

¹⁹⁰ Герасимов Б. ВИМИ — 30 лет / ИР. — 1998. — №5. — С. 30—31; Информационные ресурсы России: Национальный доклад.

¹⁹¹ Информационные ресурсы России: Национальный доклад.

¹⁹² Батенко А.И., Федоров В.И. Нормативно-методическое обеспечение межгосударственного обмена научно-технической информацией между странами Содружества Независимых Государств // НТИ. — 1998. — №8. — С. 26 — 31.

¹⁹³ Там само; Подольська В.О., Хоменко Н.В. Стратегічний аналіз — основний елемент розробки системи цілей на довгострокову експертизу // Наук, вісник ПКІ. — 2000. — №1. — С 75 — 79.

¹⁹⁴ Анфилов В.С. и др. Системный анализ в управлении: Учеб. пос. / В.С. Анфилов, А.А. Емельянов, АА. Кукушкин; Под ред АА. Емельянова. — М.: Финансы и статистика, 2002. — 368 с. — С.208.

¹⁹⁵ Соснін О. Стратегічний ресурс суспільства. Розвиток високих технологій — запорука індустріального статусу держави // Політика і час. — 2002. — №11. — С.53—60.

¹⁹⁶ Буренок В.М., Лавринов Г.А., Кравчук П.В. О возможном подходе к определению стоимости научно-исследовательских работ // Военная мысль. — 2003. — №2. — С.31 — 33.

¹⁸⁷ Закон України «Про інформацію». — Ст. 54.

¹⁹⁸ Кучма Л.Д. Три рівні стратегічного прогнозування: Виступ на засіданні Держ. комісії з питань екон. і соц. розвитку, 18 лютого 2002 р. // Урядовий кур'єр. — 2002. — 19 лют.

¹⁹⁹ Гальчинський А. Демократію — для всіх // День. — 2002. — 20 бер.

²⁰⁰ Глобалізація і безпека розвитку: Моногр. / О.Г. Білорус, Д.Г. Лук'яненко, М.О. Гончаренко та ін. — К.: КНЕУ, 2001. — 733 с — С.689 — 692.

²⁰¹ Харитончук М.В. Децентралізація державного управління як чинник демократизації суспільних відносин. — К.: ІПЕД НАНУ, 2000. — 59 с; Гриценко А.А. Економічні трансформації і перехід до нового типу розвитку: Матеріали наукової конференції «Україна на порозі ХХІ століття». — 15—16 листопада 2000 р. — К.: НТУ «КПБ», 2000. — С- 88 — 91; Зверьчцов М.І. Удосконалення управління трансформаційними процесами в Україні // Там само. — С. 93—96; Хмільовський В.М. Середній клас та громадські об'єднання підприємців — визначальний фактор соціального клімату в суспільстві // Там само. — С. 123—128; Харитончук М.В. Зарубіжні концепції і практика децентралізації державного управління: Автореф. дис. на здобуття наук. ступ. канд. політ, наук. / НАН України. Інститут світової економіки і міжнар. відносин. — К., 2000. — 17 с

²⁰² *Глобалізація і безпека розвитку: Моногр. / О. Г. Білорус, Д. Г. Лук'яненко, М. О. Гончаренко та ін. — К: КНЕУ, 2001. — 733 с — С.51 — 52.*

²⁰³ *Там само. — С 722 — 725.*

²⁰⁴ *Закон України «Про інформацію». — Ст. 30.*

²⁰⁵ *Антопольский А.А. Информационные ресурсы как объект имущественных прав // НТИ. — 1997. — №1. — С. 21—24.*

²⁰⁶ *Там само.*

²⁰⁷ *Victor Montviloff. National Information Policies: A Handbook on the Formulation, Approval, Implementation and Operation of National Policy on Information. — UNESCO. — 1990; Доти Ф. и Эрделеа С. Обзор и анализ избранных средств реализации федеральной политики в области научно-технической информации (НТИ) в 1945—1987 гг. // Политика в области научно-технической информации США / Под ред. Ч.Р.Макклур и П.Хермона. — Норвуд, 1989. — 360 с.(На англ. яз.).*

²⁰⁸ *Блер А. Зростає інвестування у британську науку. [Передова] // Сайенс (Science). — 1998. — 21 серп.; Правила Комісії Європейського Співтовариства про застосування ст.85 (3) Римської угоди щодо патентних ліцензійних угод. (№2349/84); Правила Комісії Європейського Співтовариства про застосування ст.85 (3) Римської угоди відносно ноу-хау (№556/89).*

²⁰⁹ *Правила Комісії Європейського Співтовариства про застосування ст.85 (3) Римської угоди відносно патентних ліцензійних угод. (№2349/84); Правила Комісії Європейського Співтовариства про застосування ст.85 (3) Римської угоди відносно ноу-хау (№556/89).*

²¹⁰ *Бишоп Э. и О'Нилл М. Deskriptivnyy analiz osnovnykh issledovaniy politiki nauchnoy i tekhnicheskoy informatsii // Politika v oblasti nauchno-tekhnicheskoy informatsii SSHA: vzglyady i perspektivy / Pod red. Ch.P.Makklyur i P.Xernona. — Norvud, 1989. — С. 360. (На англ. языке).*

²¹¹ *Там само.*

²¹² *Белов Г.В. Правовые аспекты формирования и использования НТИ // НТИ. — 2001. — №2 — С. 52 — 60; Балаба ВЯ. Щодо окремих проблем захисту інформаційних ресурсів України: Матеріали «круглого столу» «Захист інформаційних ресурсів в інформаційно-телекомунікаційних системах», Київ, 23.05.2001. — К.: ДСТСЗІ СБ України, 2001. — С.104 — 107.*

²¹³ *Вирковский В.А. О расширении использования информационных материалов ограниченного доступа с учетом конверсии // ВЗИ. — 1994. — №2. — С.34 — 55; Щур ГЛ. Расширение использования информационных материалов ограниченного доступа с учетом конверсии российского оборонного комплекса // МИС. — ВИМИ. — 1994. —*

№3 — 4. — С. 53 — 55; Соснн О.В. Система забезпечення інформаційної безпеки України: Аналіт. записка ШСД. — К.: НІСД, 2001- — 14 с

²¹⁴ *Там само.*

²¹⁵ *Прокоф'єв М. Підходи щодо захисту інформаційних ресурсів в інформаційно-телекомунікаційних системах: Матеріали «круглого столу» «Захист інформаційних ресурсів в інформаційно-телекомунікаційних системах», Київ, 23.05.2001. — К.: ДСТСЗІ СБ України, 2001. — С 72 — 75.*

²¹⁶ *Балаба ВЛ. Щодо окремих проблем захисту інформаційних ресурсів України: Матеріали «круглого столу» «Захист інформаційних ресурсів в інформаційно-телекомунікаційних системах», Київ, 23.05.2001. — К.: ДСТСЗІ СБ України, 2001. — С.104 — 107; Соснн ОВ. Наука та інформаційні ресурси в контексті національної безпеки: Матеріали «круглого столу» «Захист інформаційних ресурсів в інформаційно-телекомунікаційних системах», Київ, 23.05.2001. — К.: ДСТСЗІ СБ України, 2001. — С.42 — 49.*

²¹⁷ *Соснн О.В. Про правові основи удосконалення системи державного управління інформаційними ресурсами // Держава і право. — 2002. — Вип.№15. — С 196.*

²¹⁸ *Стратегія розвитку України: теорія і практика: Моногр. / За заг. ред. О. С Власюка. — К.: НІСД, 2002. — 864 с — С. 655.*

²¹⁸ *Закон України «Про інформацію».*

²²⁰ *Закон України «Про державну таємницю».*

²²¹ *Закон України «Про інформацію». — Ст. 29.*

²²² *Там само. — Ст. 30.*

²²⁸ *Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації: Затверджена постановою Кабінету Міністрів України від 27.11.98 №1893// Офіційний вісник України. — 1998. — №48. — С.31—51. — П.34.*

²²⁴ *Закон України «Про державну таємницю». — Ст. 27.*

²²⁵ *Талі салю. — Ст. 22.*

²²⁶ *Там само. — Ст. 27.*

²²⁷ *Закон України «Про захист інформації в автоматизованих системах» від 5 липня 1994 р. // Закони України / Верховна Рада України; Ін-т законодавства. — К.: Книга, 1996. — Т.7. — С.296—301.*

²²⁸ *Лапко О. Інноваційна діяльність в системі державного регулювання: Моногр. — К: Інститут економічного прогнозування НАНУ, 1999,— 253 с*

²²⁹ *Доброе Г.М. Наука: информация и управление (Информационные проблемы управления наукой). — М.: Сов. Радио, 1977. — 256 с; Развитие информатизации в Украине: 36. — К.: Держкомстат України, 2000. — 74 с; ДСТУ 3973-2000. Система розроблення та поставлення продукції на виробництво. Правила виконання науково-дослідних робіт.*

Загальні положення: Затверджено та введено в дію наказом Держстандарту України від 27 листопада 2000 р. № 677. — К.: Держстандарт України, 2000. — С.18; ДСТУ 3974-2000. Система розроблення та поставлення продукції на виробництво. Правила виконання дослідно-конструкторських робіт. Загальні положення: Затверджено та введено в дію наказом Держстандарту України від 27 листопада 2000 р. № 677. — К.: Держстандарт України, 2000. — С.34; Подольский В., Дик В., Уринцов А. Информационные системы бухгалтерского учета. — М.: Аудит — ЮНИТИ, 1998. — 319 с.

²³⁰ Серпилина Е.Ю., Хименко О.А. Организационно-правовые аспекты использования информационного ресурса государства / VIII Міжнародна науково-практична конференція: «Інформаційні ресурси НТІ: проблеми створення і використання», 30—31 травня 2001 р. — К: УкрІНТЕІ, 2001. — С.114—117.

²³¹ Крижанівський О. Обов'язок держави — захистити ефективно-го власника прав на ОІВ // ІВ, — 2001. — №11. — С.49—55.

²³² О государственной политике по вовлечению в хозяйственный оборот результатов научно-технической деятельности и объектов интеллектуальной собственности в сфере науки и технологий: Указ Президента Российской Федерации от 22.07.98 №863 // Собр. Законодат. РФ. — 1998. — №30. — Ст.3756; Об использовании результатов научно-технической деятельности: Постановление Правительства Российской Федерации от 02.09.99 №982.

²³³ Разработка типовых условий использования государственных ресурсов научно-технической информации коммерческими и некоммерческими организациями разных типов: Отчет по теме «Разработка концепции и пакета нормативно-методических документов по регулированию экономических и имущественных отношений в области информационных ресурсов ГСНТИ». — М.: НТЦ «Информрегистр», 2000.

²³⁴ Проблеми введення об'єктів інтелектуальної власності в господарчий обіг та шляхи їх вирішення: Тези доповідей 5-го галузевого семінару, Київ, 16 жовт. 2001 р. — К: МОН України, 2001.

²³⁵ Проект Закону України «Про внесення змін до Закону України «Про власність» в ред. Міністерства освіти і науки України від 19.09.2001р. №1/12-2461. —Машинопис.

²³⁶ Крижанівський О. Обов'язок держави — захистити ефективно-го власника прав на ОІВ // ІВ, — 2001. — №11. — С.49—55.

²³⁷ Андрущук Г. Інноваційна діяльність в Україні: економічний механізм стимулювання // ІВ, — 2000. — №12. — С.23—30.

²³⁸ Там само. — С 29.

²³⁹ Положення (стандарт) бухгалтерського обліку. Розд. 8: Нематеріальні активи.

20 дс ТУ 3973-2000. Система розроблення та поставлення продукції на виробництво. Правила виконання науково-дослідних робіт. Загальні положення: Затверджено та введено в дію наказом Держстандарту України від 27 листопада 2000 р. № 677. — К: Держстандарт України, 2000. — С.18; ДСТУ 3974-2000. Система розроблення та поставлення продукції на виробництво. Правила виконання дослідно-конструкторських робіт. Загальні положення: Затверджено та введено в дію наказом Держстандарту України від 27 листопада 2000 р. №677. — С.34.

²⁴¹ Мітрахович М. Охорона об'єктів промислової власності воєнного призначення // ІВ, — 2000. — №9-10. — С.56-59. — С 56.

²⁴² Там само. — С 57.

²⁴³ Хойер В. Как делать бизнес в Европе. — М.: Прогрессе, 1999. — 253 с.; Белов Г.В., Нечипоренко В.П., Косарев А.С. Реорганизация предприятий научно-технической сферы и правовые проблемы сохранения информационных ресурсов научно-технической информации // ПИ. — 1999. — №3. — С.94—96; Козырев А.Н. Оценка интеллектуальной собственности. — М.: Экспертное бюро, — 1997. — 289 с; Гарнер Д., Оуэн Р., Конвей Р. Пособие Эрнст энд Янг. Привлечение капитала / Пер. с англ. — М.: «Джон Уайтли энд Санз», 1995; Коммерциализация интеллектуальной собственности: проблемы и решения / Сост. и общ. ред. Н. М. Фонштейн и В. Г. Зиновьева. — С.58—71.

²⁴⁴ Козырев А.Н. Общее равновесие в экономике с рынками продуктов и лицензий: Тез. докл. Всесоюзн. семинара «Социально-экономич. процессы». — Кишинев, 1989. — С.163—164.

²⁴⁵ Леонтьев В. О передаче патентных прав на изобретения, сделанные в ходе исследований по заказам правительства // Экономическое эссе. Теории, исследования, факты и политика / Пер. с англ. — М.: Политиздат, 1990. — 414 с; Коуз Р. Фирма, рынок и право. — М.: Дело, 1993. — 192 с.

²⁴⁶ Про державну реєстрацію та облік НДДКР та дисертацій закритої тематики: Постанова Кабінету Міністрів України від 10.03.94 р. №155. — Чинна з 10 березня 1994 р.; Про державну реєстрацію НДДКР та дисертацій відкритої тематики: Постанова Кабінету Міністрів України від 31.03.92 р. №162. — Чинна з 31 березня 1992 р.

²⁴⁷ Белов Г.В., Нечипоренко В.П., Косарев А.С. Реорганизация предприятий научно-технической сферы и правовые проблемы сохранения информационных ресурсов научно-технической информации // ПИ. — 1999. — №3. — С.94—96; Бухгалтерський облік на підприємствах України з різними формами власності. ЧИ. Розділ 2.13: Нематеріальні активи, їх облік.

²⁴⁸ Хурматуллин В.В. Интеллектуальная собственность как нематериальные активы // НТИ. — 1997. — №1. — С.19—21. — С.19.

²⁴⁶ Симонова Л.М. Оцінка нематеріальних активів в умовах економіки перехідного періоду // Оцінювач. — 1997. — №7. — С.44—46; *Порядок* експертної оцінки нематеріальних активів: Затверджено наказом ФДМ та Держкомітету з питань науки і технологій від 27.07.1995. № 969/97. — К.: ФДМ України, 1995; Как идею превратить в товар // Поиск. — 1999. — №49; *Макуха В.В.* Особливості оцінки заставної нерухомості // Оцінювач. — 1999. — №12. — С.69—70; *Томас Пол Р.* Учебный пример оценки стоимости нематеріальних активів — ліцензії на здійснення діяльності в області телекомунікацій // Вісник оцінки. — 1997. — Вип.6. — С.2—5; *Городов О.* О залоге прав на изобретение // Интеллектуальная собственность. — 2000. — №11—12. — С.20—23; *Симонова Л.М.* Оцінка застави // Вісник оцінки. — 1997. — №7—8. — С.2—6; *Оценка* ссудного обеспечения, залога и долговых обязательств. Международные стандарты оценки МСО 1—4. Международный комитет по стандартам оценки имущества. Российское общество оценщиков. — М., 1995; *Оценка* интеллектуальной собственности. Стандарт Российского общества оценщиков // Вісник оцінки. — 1997. — №3—4; *Стандарты* оценки нематериальных активов // Международные стандарты оценки МСО 1—4. — М.: РОО, 1995. — Т.1.

²⁵⁰ *Порядок* експертної оцінки нематеріальних активів: Затверджено наказом ФДМ та Держкомітету з питань науки і технологій від 27.07.1995. № 969/97.

²⁵¹ *Подольский В., Дик В., Уринцов А.* Информационные системы бухгалтерского учета. — М.: Аудит — ЮНИТИ, 1998. — 319 с; *Дяків Т., Чуєв М.* Оцінка нематеріальних активів — чий це клопіт? // ІВ. — 2001. — №3. — С.16—18.

²⁶² Там само. — С 16.

²⁶³ *Коуз Р.* Фирма, рынок и право. — М.: Дело, 1993. — 192 с; *Дяків Т., Чуєв М.* Бухгалтерський облік витрат на рекламу очима патентознавця // ІВ. — 2000. — №8—9. — С.58—61.

²⁵⁴ Закон України «Про охорону прав на винаходи та корисні моделі» // Відомості Верховної Ради України. — 1994. — №7.

²⁵⁵ *Концепция* использования результатов научно-технической деятельности, созданных за счет средств федерального бюджета // МИС. — ВИМИ. — 1997. Вып.1—2. — С.30—36.

²⁵⁶ *Козырев А.Н.* Алгебраические свойства информации и рынок // НТИ. — 1999. — №5. — С.15—20.

²⁵⁷ *Кому* владеть интеллектуальной собственностью // Поиск. — 1997. — №8. — 22 февр.; *Продав* информацию — получи статью // Поиск. — 1997. — №11. — 15 марта.

²⁵⁸ *Козырев А.Н.* Алгебраические свойства информации и рынок // НТИ. — 1999. — №5. — С.15—20; *Козырев А.Н.* Общее равновесие в экономике с рынками продуктов и лицензий: Тез. докл. Всесоюз. семи-

нара «Социально-экономич. процессы». — Кишинев, 1989. — С.163—164; *Adelstein R., Peretz S.I.* The competition of technologies in market for ideas: copyright and fair use in evolutionary perspective // International Review of Law and Economics. — 1985. — №5. — P.209—238.

²⁵⁹ *Шнак А.П.* Передача технологий в Україні: ситуація і проблеми // Наука та наукознавство. — 2000. — №1—2. — С. 14—20.

²⁶⁰ *Баряхтар В.* Глобализация, развитие общеевропейского научного пространства и проблемы защиты национальных интересов в области интеллектуальной собственности и информационной безопасности: Материалы междунар. симпозиума, Киев 22—25 сентября 2001 г. — К.: УАННП «Феникс». — 2002. — С.313—314.

²⁶¹ Про *порядок* оформлення і використання прав на винаходи, корисні моделі і промислові зразки: Положення затверджене Постановою Верховної Ради України 19 січня 1995 р. // Голос України. — 1995. — 14 лют.

²⁶² *Белое В.В.* Проблемы охраны интеллектуальной собственности // НТИ. — 1997. — №1 — С.15—18.

²⁶³ *Коммерциализация* интеллектуальной собственности: проблемы и решения / Сост. и общ. ред. Н. М. Фонштейн и В. Г. Зиновьева. — С.58—71; *Белое В.В.* Проблемы охраны интеллектуальной собственности. — С.15—18; *Интеллектуальна* власність в Україні: Реєстрація договорів про передачу прав на об'єкти промислової власності / Л.І.Ніколаєнко та ін. / За ред. ВЛ.Петрова. — К, 1999. — 48 с; *Попов М.И.* Системный анализ норм законодательства России, регулирующего деятельность в области коммерческого оборота «ноу-хау» // Правовая информатика. — 1996. — №1.

²⁶⁴ *Конституція* України // Закони України / Верховна Рада України; Ін-т законодавства. — К.: Книга, 1997. — ТЛО. — С.5—40.

²⁶⁵ Закон України «Про власність» від 7 лютого 1991 р. // Закони України / Верховна Рада України; Ін-т законодавства. — К.: Книга, 1996. — Т.1. — С.173—188.

²⁶⁶ Закон України «Про державну таємницю» в ред. від 21 вересня 1999 р. // Голос України. — 1999. — 26 жовт.

²⁶⁷ Про *порядок* оформлення і використання прав на винаходи, корисні моделі і промислові зразки: Положення затверджене Постановою Верховної Ради України 19 січня 1995 р. // Голос України. — 1995. — 14 лют.

²⁶⁸ Закон України «Про державну таємницю». — Ст. 3.

²⁶⁸ *Методичні* рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності: Затверджено наказом Дер-

жкомсекретів України від 09.02.98, №23. 36. №8. — К: Держкомсекретів України, 1998. — С.4—24.

²⁷⁰ *Секретна інформація в сфері національної безпеки*. Директива Президента США від 04.95, №12958. 36 №19. — К.: Держкомсекретів України, 1999. — С.2—27.

²⁷¹ *Закон Российской Федерации «О государственной тайне»*. — С.279—301.

²⁷² *Закон України «Про державну таємницю»*.

²⁷³ *Там само.*

²⁷⁴ *Там само.*

²⁷⁵ *Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності*: Затверджено наказом Держкомсекретів України від 09.02.98, №23. 36. №8.

²⁷⁶ *Звід відомостей, що становлять державну таємницю*. Затверджено наказом СВ України від 01.03.2001, №52. — Чинний з 13.04.2001.

²⁷⁷ *Загсом України «Про наукову і науково-технічну експертизу»* // Голос України. — 1999. — 26 жовт.

²⁷⁸ *Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності*: Затверджено наказом Держкомсекретів України від 09.02.98, №23. 36. №8.

²⁷⁹ *Закон України «Про державну таємницю»*.

²⁸⁰ *Звід відомостей, що становлять державну таємницю*: Затверджено наказом СВ України від 01.03.2001, №52. — Чинний з 13.04.2001.

²⁸¹ *Там само.*

²⁸² *Чумаченко Б., Лавров К.* Международный трансфер технологий: опыт американских корпораций // Проблемы теории и практики управления. — 1999. — №2. — С.3—14; *Разработка* типовых условий использования государственных ресурсов научно-технической информации коммерческими и некоммерческими организациями разных типов: Отчет по теме «Разработка концепции и пакета нормативно-методических документов по регулированию экономических и имущественных отношений в области информационных ресурсов ГСНТИ». — М.: НТЦ «Информрегистр», 2000; *Зинов В., Сафарян К.* Интеллектуальный капитал как базовая характеристика стоимости бизнеса // IB. — 2000. — №5—6. — С.23—35; *Committee to Study International Developments in Computer Science and Technology.* Global trends in computer technology and their impact on export control. Washington: National Academy Press. 1998. — P.171; *Crabher G.* Eastern conquest — the «transcated industrialization» of East European regions by large western corporations. In: H.Ernste, V.Mejer. Regional development and

contemporary industrial response. London: Belhaven Press, 1991. — P.141—212.

²⁸³ *Лопатин В.Н.* Безопасность экономики информационных технологий в условиях глобализации // ПИ. — 2001. — Вып.2. — С.10—21; *Новосельцева О.* Аудит интеллектуальной собственности при оценке нематериальных активов // Финансовая газета. — 1996. — №47; Проект книги 4 Цивільного кодексу «Право інтелектуальної власності» // IB. — 2000. — №8—9. — С. 78—82.

²⁸⁴ *Бачило И.Л.* Информационные технологии в структуре экономики Российской Федерации // Проблемы информатизации. — 2001. — Вып.2. — С. 3—9; *Козырев А.* Интеллектуальная собственность в хозяйственном обороте // Содружество. — 2000; *Нечипоренко В.П., Полунина Т.К., Цветкова В.А.* Некоторые итоги анализа информационной инфраструктуры России / 5-я Юбил. междунар. конф.: «Библиотеки и ассоциации в меняющемся мире: новые технологии и новые формы сотрудничества». Крым — 98, Респ. Крым. Украина, Судак, 6—14 июня. — 1998. — Т.2. — С.392—394.

²⁸⁵ *Макаренко С.А.* Идеология информационного общества та правові проблеми інформаційного поля // Актуальні проблеми міжнародних відносин. — К., 1999. — Вип.14. — 4.1; Мергсер *Гютер*. Практикоорієнтована сучасна концепція управління державним сектором // Актуальні проблеми міжнародних відносин. — К., 2000. — Вип. 16. — 4.1. — С.163—172.

²⁸⁶ *Кучма Л.Д.* Україна: підсумки соціально-економічного розвитку та погляд в майбутнє: Виступ Президента України Л. Д. Кучми на науковій конференції «Україна на порозі ХХХІ століття: уроки реформ та стратегія розвитку», Київ, 16 листопада 200 р. // Стратегічна панорама. — 2000. — №3—4. — С.3—20.

²⁸⁷ *Панастогс Б.* Основи ідеології суспільного життя // Економіка України. — 1999. — №12. — С.12.

²⁸⁸ *Мочерний С.* До концепції соціально-економічного розвитку України // Економіка України. — 1996. — №5. — С.54.

²⁸⁹ *Кравченко І.* Українська кооперативна держава // Літературна Україна. — 1995. — 21 грудня. — С.5.

²⁹⁰ *Черняк В.* Модель економіки: вибір України // Економіка України. — 1995. — №9. — С.32.

²⁹¹ *Мамутов В.К.* Економіко-правовые аспекты развития хозяйственного комплекса // Матеріали наук. конф. «Україна на порозі ХХІ століття: уроки реформ та стратегія розвитку», Київ, 15—16 листопада 2000 р. / Україна на порозі ХХІ століття. — К.: НТУ «КПІ», 2000. — СІЮ.

²⁹² *Там само.*

²⁹³ *Врятування у Сполучених Штатах. Нарис.* — Інформаційне агентство Сполучених Штатів. — Оригінальне видання Ричарда Шредера. — RPO 9404-051 UKRAINIAN.

²⁹⁴ РЖ ВИНІТИ Інформатика. — 1994. — № 3—6. — Реф. 37—40. — Бібл. — 125 найм.

²⁹⁵ *Там само.*

²⁹⁶ *Об общегосударственной системе научно-технической информации: Постановление Совета Министров СССР от 29 ноября 1966 г.* № 916.

²⁹⁷ *Закон України «Про науково-технічну інформацію».*

²⁹⁸ РЖ ВИНІТИ Інформатика. — 1994. — № 3—6. — Реф. 37—40.

²⁹⁹ *Актуальні питання методології та практики науково-технологічної політики / За ред. Б.А. Малицького. Центр доел, науково-техн. потенціалу та історії науки ім. Г. М. Доброва НАНУ.*

³⁰⁰ *World Information Report 1997/98.* — UNESCO Publishing. UNESCO, Paris, 1998.

³⁰¹ *Макаренко Є.А. Інформаційне суспільство, політика, право в програмній діяльності ЮНЕСКО.* — К.: Наша культура і наука, 2002; *World Information Report 1997/98.* — UNESCO Publishing. UNESCO, Paris, 1998; *Решения ЮНЕСКО 1996—1997 гг.* // <http://www.unesco.org/publishing>.

³⁰² *Макаренко Є.А. Інформаційне суспільство, політика, право в програмній діяльності ЮНЕСКО.* — К.: Наша культура і наука, 2002. — С. 85.

³⁰³ *Талі само.* — СІ02.

³⁰⁴ *Там само.* — С. 349—358.

⁸⁰⁵ *Хохлов М. Про економічний зміст категорії власності в транзитивній економіці // Економіст.* — 2000. — № 1. — С. 36—43; *Савин А.Н. Может ли научно-техническая информация приносить доход? // НТИ.* — 1998. — № 11. — С. 18—19.

³⁰⁶ *Доброе Г.М. Наука: информация и управление (Информационные проблемы управления наукой).* — М.: Сов. Радио, 1977. — 256 с. (Бібл. — 203 наймен.).

³⁰⁷ *Кедровский О.В. Информационное пространство России // МИС.* — 1994. — № 3—4. — С. 12; *Антопольский А. Б. Проблемы государственного регулирования информационной деятельности // ИРР.* — 1998. — № 3. — С. 18—21.

³⁰⁸ *Нечипоренко В.П., Полунина Т.К., Цветкова В.А. Некоторые итоги анализа информационной инфраструктуры России / 5-я Юбил. междунар. конф.: «Библиотеки и ассоциации в меняющемся мире: новые технологии и новые формы сотрудничества».* Крым — 98, Респ. Крым, Украина, Судак, 6—14 июня.

³⁰⁹ *Котлер Ф. Основы маркетинга / Пер. с англ.* — М.: Прогресс, 1990. — С. 399—404; *Нечипоренко В.П., Полунина Т.К., Цветкова В.А. Некоторые итоги анализа информационной инфраструктуры России / 5-я Юбил. междунар. конф.: «Библиотеки и ассоциации в меняющемся мире: новые технологии и новые формы сотрудничества».* Крым — 98, Респ. Крым, Украина, Судак, 6—14 июня; *Подольська В.О., Хоменко Н.В. Стратегічний аналіз — основний елемент розробки системи цілей на довгострокову експертизу // Наук, вісник ПКІ.* — 2000. — № 1. — С. 75—79; *Ильин А.М. Планирование на предприятии.* — Изд. 1: *Стратегическое планирование: Учеб. пос.* — Минск: Мисанта, 1998. — 294 с.

⁸¹⁰ *Нечипоренко В.П. Информационный капитал научно-технической деятельности // НТИ.* — Сер. 1. — 1998. — № 11 — С. 2—8; *Савин А.Л. Может ли научно-техническая информация приносить доход? // НТИ.* — 1998. — № 11. — С. 18—19; *Кедровский О.В. ГСНТИ: центр и регионы // НТИ.* — 1998. — № 11. — С. 10—11.

³¹¹ *Правове регулювання інформаційної діяльності в Україні / Упор. Є. Демський. Відп. ред. С. Павлюк.* — К.: Юринком, 2001. — 688 с.

⁸¹² *Кедровский О.В. ГСНТИ: центр и регионы.*

⁸¹⁸ *Везиров В.Н., Полтев А.А. ВИМИ и его место в системе ГСНТИ / НТИ.* — 1998. — № 11. — С. 29—31.

⁸¹⁴ *Положение о государственной службе научно-технической информации: Постановление Правительства Российской Федерации от 25.07.97 г. № 950 // НТИ.* — 1997. — № 11. — С. 24—26.

⁸¹⁵ *Бармин Л.В., Степанов В.Е. Информационно-аналитическая поддержка развития и использования двойных технологий // МИС.* — 1994. — № 3—4. — С. 58—61.

³¹⁶ *Соснін О.В. Проблемні питання захисту і раціонального використання інформаційних ресурсів оборонного промислового комплексу України в процесі інтеграції до Європейського Союзу: Аналіт. матеріали ШСД.* — К.: ШСД, 2002. — С. 2—8.

⁸¹⁷ *Антопольский А.Б. Проблемы государственного регулирования информационной деятельности // ИРР.* — 1998. — № 3. — С. 18—21; *Разработка типовых условий использования государственных ресурсов научно-технической информации коммерческими и некоммерческими организациями разных типов: Отчет по теме «Разработка концепции и пакета нормативно-методических документов по регулированию экономических и имущественных отношений в области информационных ресурсов ГСНТИ».* — М.: НТЦ «Информрегистр», 2000.

³¹⁸ Антопольский А.Б. Проблемы государственного регулирования информационной деятельности.

³¹⁹ Проект Закону України «Про інформаційний суверенітет та інформаційну безпеку». Внесено на розгляд Верховної Ради України 7 липня 1998 р.; Проект Концепції реформування законодавства у сфері суспільних інформаційних відносин: Матеріали «круглого столу» «Захист інформаційних ресурсів в інформаційно-телекомунікаційних системах», Київ, 23 травня 2001 р. — К.:ДСТЗІ СВ України, 2001. — С.86—94; Закон України «Про державну таємницю»; Концепція (Основи державної політики) національної безпеки України. Схвалена Постановою Верховної Ради України 16 січня 1997 р. №3/97 — ВР. — Урядовий кур'єр. — 1997. — 6 лют.

³²⁰ Морозов И. Л. Информационная безопасность политической системы // Полис. — 2002. — №5. — С.134—144.

³²¹ Проект Концепції реформування законодавства у сфері суспільних інформаційних відносин: Матеріали «круглого столу» «Захист інформаційних ресурсів в інформаційно-телекомунікаційних системах», Київ, 23 травня 2001 р. — К.:ДСТЗІ СВ України, 2001. — С.86—94.

³²² Волокитин А.В., Копылов В.А. Информационная безопасность и информационное законодательство // НТИ. — 1996. — №7. — С.1—3.

³²³ Кристальный Б.В. Вопросы информационного законодательства в свете принятия России в Совет Европы // НТИ. — 1996. — №7. — С.3—9.

³²⁴ Мамонов Н.Е. Перспективы применения термина «служебная тайна» в законодательных актах по проблеме защиты информации // НТИ. — 1996. — №7. — С.25—28.

³²⁵ Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації: Затверджена постановою Кабінету Міністрів України від 27.11.98 №1893 // Офіційний вісник України. — 1998. — №48. — С.31—51.

³²⁶ Мамонов Н.Е. Перспективы применения термина «служебная тайна» в законодательных актах по проблеме защиты информации.

³²⁷ Проект Концепції реформування законодавства у сфері суспільних інформаційних відносин: Матеріали «круглого столу» «Захист інформаційних ресурсів в інформаційно-телекомунікаційних системах».

³²⁸ Секретна інформація в сфері національної безпеки. Директива Президента США від 04.95, №12958. 36. №19. — К: Держкомсекретів України, 1999. — С.2—27.

³²⁹ Закон Российской Федерации «О государственной тайне» от 21 июля 1993.

³³⁰ Закон Китайской Народной Республики «О соблюдении государственной тайны» от 5 сентября 1988 г. — Ст. 8 // Сб. норм. док. №19. — К.: Держкомсекретів України, 1999. — С.28—36.

³³¹ Заком України «Про державну таємницю». — Ст.8.

³³² Там само.

³³³ Там само. — Ст. 19.

³³⁴ Там само. — Ст. 6.

³³⁵ Там само. — Ст. 1.

³³⁶ Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності: Затверджено наказом Держкомсекретів України від 09.02.98, №23. 36. №8.

³³⁷ Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації: Затверджена постановою Кабінету Міністрів України від 27.11.98 №1893 // Офіційний вісник України. — 1998. — №48. — С.31—51.

³³⁸ Додонов О. Г., Литвиненко О. В., Янгиевський С. О. Інформаційна політика органів державної влади // Стратегії розвитку України: теорія і практика / За заг. ред. О. С Власюка. — К: НІСД, 2002. — С.636—650.

³³⁹ Там само. — С 646—648.

³⁴⁰ Макаренко Є.А. Інформаційне суспільство, політика, право в програмній діяльності ЮНЕСКО; Clark D. Post-Industrial America: an Geographical Perspective. — N.Y. — L., 1985; Kahn H., Brow W., Martel L. The next 200 Years. A Scenari for America and the World. — N.Y., 1971; Naisbitt T. Global Paradox. — NY., 1995; Dordick H., Wang G. The Information Society: a Retrospective View. — L.: Newbury Park, 1963; Garnham N. Capitalism and communication: Global culture and the economics of information. — London: Sage, 1994; Information Society: Agenda for Action in the UK. — L., 1996; Todd Keith. Up to the Information Society, <http://www.isi.gov.uk>; Мелюхин И.С. Информационное общество: истоки и проблемы. — М.: МГУ, 1999; Building the European information Society for US All. First Reflections of the High Level Group of Experts. Interim Report. — Brusseles, 1996; Eropean Way to the information Society: An Action plan by the European Commission. — Brusseles, 1994; Ewrope and Global information Society to the Corfu European Council (Bangeman Group). European Comission, 1994; Datton W., Blumler T., Garnham N. et all. The Politics of information and Communication Policy: The information Superhighway // Information and Communicassion Technologies. Visions and Realities / Ed. by William Dutton. — Oxford: Oxford University Press, 1996; Virtual New World? — Strasbourg, Council of Europe Publishing, 1998; Report on Europe Scientific and Technological Cooperation: Towards A New Institutional Framework. — Strasbourg, 1997. — Doc.5784. — Annex «А». P. B. T; Nora S., Mine A. The Computerisation of Society. A Report

to the President of France. Cambridge. — L., 1996; *Developing Finnish information Society/ Decision in Principle*. — Helsinki, 1995.

³⁴¹ *Мастяниця Й.У., Соснін О.В., Шиманський Л.Є.* Проблеми формування функціональної організаційно-правової системи управління національними інформаційними ресурсами України / Аналітичні матеріали НІСД; *Олійник О.В., Соснін О.В., Шиманський Л.Є.* Політико-правові аспекти формування інформаційного суспільства суверенної і незалежної держави // *Держава і право*. — 2001. — Вип.12. — С.534—541.

³⁴² *Конституція України.*

³⁴³ *Проект Концепції реформування законодавства у сфері суспільних інформаційних відносин: Матеріали «круглого столу» «Захист інформаційних ресурсів в інформаційно-телекомунікаційних системах», Київ, 23 травня 2001 р.*

³⁴⁴ *Проект Інформаційного кодексу України. Перша редакція проекту.*

³⁴⁵ *Проект Закону України «Про національні інформаційні ресурси» (на стадії узгодження).* — К.: Держкомзв'язку та інформатизації України, 2001. — Машинопис.

³⁴⁶ *Мастяниця Й.У., Соснін О.В., Шиманський Л.Є.* Проблеми формування функціональної організаційно-правової системи управління національними інформаційними ресурсами України / Аналітичні матеріали НІСД; *Мастяниця Й. У., Соснін О. В., Шиманський Л. Є.* Інформаційні ресурси України: проблеми державного управління / За заг. ред. О. В. Сосніна;

³⁴⁷ *Закон України «Про державну таємницю».*

³⁴⁸ *Там само.* — Ст. 19.

³⁴⁹ *Шаваев А.Г.* Система борьбы с экономической разведкой. — М.: Правовое просвещение, 2000. — С. 16, 23.

³⁵⁰ *Багиров А.* Новые информационные технологии в международных отношениях // *Международная жизнь*. — 2001. — №6. — С.90—96.

³⁵¹ *Бачило И. Л.* Информационное право, роль и место в системе права Российской Федерации // *Государство и право*. — 2001. — №2. — С.5—14.

³⁵² *Мусиенко І.В.* Наказуемая неосторожность в печати / Сравнение русских, французских и немецких законов о печати. — Одесса, 1915.— СПб.

³⁵³ *Там само.* — С. 20—23.

³⁵⁴ *Корольке ВТ.* Основы Паблик Рилейшнз. — К.: Ваклер, 2001. — С. 11.

³⁵⁵ *Горбатюк О.М.* Політичний менеджмент інформаційної безпеки України // Київський національний університет ім. Т. Шевченка. Вісник «Міжнародні відносини». — К, 2001. — Вип.19. — *СЮ.*

³⁵⁶ *Губерський Л.В.* На чому ґрунтується міжнародний авторитет // *Політика і час*. — 2002. — № 4. — С.11.

³⁵⁷ *Концепція (Основи державної політики) національної безпеки України, <http://guru.rada.kiev.ua:2000>].*

³⁵⁸ *Положення про порядок і механізм формування та опублікування зводу відомостей, що становлять державну таємницю: Затверджено постановою Кабінету Міністрів України від 29.04.94, № 278 // 36. норм, док., №10. — К: Держкомсекретів України, 1998. — С.16 — 18.*

³⁵⁹ *Положення про порядок і умови надання органам державної виконавчої влади, підприємствам, установам і організаціям дозволу (ліцензії) на здійснення діяльності, пов'язаної з державною таємницею та про особливий режим цієї діяльності: Затверджено постановою Кабінету Міністрів України від 20.06. 1994 р. , № 426 // 36. норм, док., №11. — К.: Держкомсекретів України, 1998. — С. 1—4.*

³⁶⁰ *Про заходи щодо виконання Постанови Верховної Ради України від 5 липня 1994 року «Про введення в дію Закону України «Про захист інформації в автоматизованих системах» та статті Закону України «Про державну таємницю»: постанова Кабінету Міністрів України від 13.01. 1995 р. , № 24 // 36. норм, док., № 4. — К.: Держкомсекретів України, 1997. — С 43—48.*

³⁶¹ *Звід відомостей, що становлять державну таємницю: Затверджено наказом Держкомсекретів України від 31.07.1995 р., №47. — Урядовий кур'єр. — 1995. — 17 серп.*

³⁶² *Положення про режимно-секретні органи в міністерствах, відомствах Автономної Республіки Крим, місцевих органах державної виконавчої влади, виконкомах Рад, на підприємствах, в установах і організаціях: Затверджено постановою Кабінету Міністрів України від 04.09. 1995 р. , № 609 // 36. норм, док., № 11. — К.: Держкомсекретів України, 1998. — С 5—12.*

³⁶³ *Положення про порядок надання, скасування та переоформлення допуску громадян України до державної таємниці: Затверджено постановою Кабінету Міністрів України від 30.07.1996 р., № 878 // 36. норм. док. — К.: Держкомсекретів України, 1998. — С. 1—15.*

³⁶⁴ *Інструкція про порядок відбору та передачі секретних документів на архівне зберігання: Затверджено наказом Держкомсекретів України і Головархіву України від 03.03.1997 р., № 25/7 // 36. норм, док., № 9. — К.: Держкомсекретів України, 1998. — С. 8—42.*

³⁶⁵ *Типове положення про секретний архівний підрозділ державного органу, підприємства, установи і організації: Затверджено наказом Держкомсекретів України і Головархівом України від 03.03.1997 р., № 26/8 // 36. норм, док., № 9. — К.: Держкомсекретів України, 1998. — С 3—7.*

³³⁰ *Нормативно-правові акти, що регулюють особливості здійснення наглядових, контрольно-ревізійних та інших функцій органів державної влади щодо підприємств, установ і організацій, діяльність яких пов'язана з державною таємницею* // 36. норм. док., № 14. — К.: Держкомсекретів України, 1999. — 16 с

⁸⁸⁷ *Концепція технічного захисту інформації в Україні*: Затверджено постановою Кабінету Міністрів України від 08.10.1997 р., № 1126 // 36. норм. док., № 4. — К.: Держкомсекретів України, 1997. — С 1—13.

³⁶⁸ *Рекомендований перелік нормативних документів системи технічного захисту інформації*: Затверджено наказом Держкомсекретів України від 22.05.1997 р., № 51 // 36. норм. док., № 7. — К.: Держкомсекретів України, 1998. — 16 а

³⁶⁸ *Яро рішення* Ради національної безпеки і оборони України від 31 жовтня 2001 року «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України: Указ Президента України від 06.12.2001, №1193.

³⁷⁰ *Секретна інформація в сфері національної безпеки*. Директива Президента США від 04.95, №12958 // 36.норм. док., №19. — К.: Держкомсекретів України, 1999. — С.2—27; *Наставление по защите секретной информации в промышленности США*. Введено в действие директивой Президента США от 08.03.72, №11652. — К.: Держкомсекретів України, 1999. — С.28—45.

⁸⁷¹ Закон Российской Федерации «О государственной тайне».

³⁷² *Общая межминистерская инструкция по защите секретов и информации, касающейся национальной обороны и государственной безопасности* от 12.03.82, №1300/SGD/SSD. Французская Республика // Сб. норм. док. — К.: Держкомсекретів України, 1998. — С.2—17.

³⁷³ *Инструкция по защите секретов в экономике ФРГ* (по состоянию на 12.02.97) // Сб. норм. док. — К.: Держкомсекретів України, 1998. — 41с.

⁸⁷⁴ Закон Китайской Народной Республики «О соблюдении государственной тайны» от 5 сентября 1988 г. // Сб. норм. док., №19. — К.: Держкомсекретів України, 1999. — С.28—36.

³⁷⁵ Закон України «Про державну таємницю».

³⁷⁶ *Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня їх секретності*: Затверджено наказом Держкомсекретів України від 09.02.98, №23 // 36.норм. док., №8. — К.: Держкомсекретів України, 1998. — С.4—24.

³⁷⁷ *Національна безпека України 1994—1996 рр.*: Наукові доповіді НІСД / Редкол: Белов О.Ф. (голова) та ін. — (Сер. «Загальноінститутські доповіді»). — К: НІСД, 1997. — С.129.

³⁷⁸ Закон України «Про державну таємницю».

⁸⁷⁹ *Соглашение о взаимном обеспечении сохранности межгосударственных секретов*: Заключено между Правительствами государств—участников СНГ 22.01.93. в г. Минске // Сб. норм. док. — К.: Держкомсекретів України, 1995. — С.1—5.

⁸⁸⁰ *Положение о порядке рассекречивания архивных документов* Правительства СССР. Утверждено постановлением Правительства Российской Федерации 22.05.95, №170 // Сб. норм. док. — К.: Держкомсекретів України, 1995. — С.12—17.

⁸⁸¹ Закон України «Про національний архівний фонд і архівні установи» від 24 грудня 1993 // Закони України / Верховна Рада України; Ін-т законодавства. — К: Книга, 1996. — Т.6. — С.387—398.

³⁸² Закон України «Про державну таємницю».

³⁸⁸ Закон. України «Про інформацію»; Закон України «Про науково-технічну інформацію»; Закон України «Про основи державної політики України у сфері науки і науково-технічної діяльності»; *Закон України «Про охорону прав на винаходи і корисні моделі»; Закон України «Про власність»* від 07 лютого 1991 р. // Закони України / Верховна Рада України; Ін-т законодавства. — К.: Книга, 1996. — Т.1. — С.173—188.

³³⁴ Закон України «Про державну таємницю».

⁸⁸⁵ Там само.

³⁸⁶ *Секретна інформація в сфері національної безпеки*. Директива Президента США від 04.95, №12958. 36.норм. док., №19. — К.: Держкомсекретів України, 1999. — С.2—27; *Наставление по защите секретной информации в промышленности США*. Введено в действие директивой Президента США от 08.03.72, №11652. — К.: Держкомсекретів України, 1999. — С.28—45.

³⁸⁷ Закон України «Про інформацію».

⁸⁸⁸ Закон України «Про державну таємницю».

³⁸⁸ Там само. — Ст.3.

⁸⁸⁰ *Звід відомостей, що становлять державну таємницю*: Затверджено наказом СВ України від 01.03.2001, №52. — Чинний з 13.04.2001.

⁸⁹¹ *Національна безпека України 1994—1996 рр.*: Наукові доповіді НІСД / Редкол: Белов О.Ф. (голова) та ін. — (Сер. «Загальноінститутські доповіді»),— С172.

⁸⁹² Закон України «Про державну таємницю». — Ст.27.

⁸⁸³ Закон України «Про інформацію».

³⁹⁴ Закон України «Про національну програму інформатизації» від 4 лютого 1998 // Закони України / Верховна Рада України; Ін-т законодавства. — К.: Книга, 1998. — Т.15. — С 134—145.

³⁹⁵ Закон України «Про інформацію».

³⁹⁶ Закон Российской Федерации «О государственной тайне»; *Федеральный Закон Российской Федерации «Об информации, информатизации и защите информации»* от 20.02.95, №24. — М.: СЗ РФ, 1995. — №8. — Ст.609; *Указ Президента Российской Федерации «Об утверждении Перечня сведений конфиденциального характера»* от 06.03.97, №188 // Защита информации. Конфидент. — 1997. — №3. — С3.

³⁹⁷ Закон України «Про інформацію».

³⁹⁸ *Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації*: Затверджена постановою Кабінету Міністрів України від 27.11.98. №1893 // Офіційний вісник України. — 1998. — №48. — С.31 — 51.

³⁹⁹ Закон України «Про інформацію».

⁴⁰⁰ Там само. — Ст.28.

⁴⁰¹ Там само. — Ст.38.

⁴⁰² Там само. — Ст.30

⁴⁰³ Там само. — Ст.30.

⁴⁰⁴ Там само. — Ст.30.

⁴⁰⁵ Там само. — Ст.46.

⁴⁰⁶ *Конвенція про захист (прав) фізичних осіб у зв'язку з автоматизованою обробкою персональних даних*. Прийнято Радою Європи 28.01.91. — Страсбург, 1991. (Сер. «Європейські Угоди», №108 (ETS108).

⁴⁰⁷ *Защита персональных данных в сфере телекоммуникационных услуг*: Рекомендации Комитета Министров Совета Европы от 07.02.95, NR(95)4. В г. Страсбурге // 36. норм. док. — К.: Госкомсекретов Украины, 1995.

⁴⁰⁸ Закон України «Про інформацію».

⁴⁰⁹ Закон України «Про державний реєстр фізичних осіб-платників податків та інших обов'язкових платежів» від 22 грудня 1994 р. // Закони України / Верховна Рада України; Ін-т законодавства. — К.: Книга, 1996. — Т.7.

⁴¹⁰ *Конвенція про захист (прав) фізичних осіб у зв'язку з автоматизованою обробкою персональних даних*. Прийнято Радою Європи 28.01.91. — Ст.5, 6.

⁴¹¹ Конституція України. — Ст. 26, 33.

⁴¹² *Конвенція про захист (прав) фізичних осіб у зв'язку з автоматизованою обробкою персональних даних*. Прийнято Радою Європи 28.01.91. — Ст.8, 14.

⁴¹³ Закон України «Про державний реєстр фізичних осіб—платників податків та інших обов'язкових платежів». — Ст. 8.

⁴¹⁴ Конституція України. — Ст. 32.

⁴¹⁵ Закон України «Про інформацію» від 2 жовтня 1992 р. // Закони України / Верховна Рада України; Ін-т законодавства. — К.: Книга, 1996. — Т.4. — С.72—78. — Ст.23.

⁴¹⁶ Там само. — Ст. 38.

⁴¹⁷ Конституція України. — Ст. 32.

⁴¹⁸ Закон України «Про інформацію». — Ст.30.

⁴¹⁹ *Конвенція про захист (прав) фізичних осіб у зв'язку з автоматизованою обробкою персональних даних*. Прийнято Радою Європи 28.01.91.

⁴²⁰ Олійник О.В., Соснін О.В., Шиманський Л.Є. Політико-правові аспекти формування інформаційного суспільства суверенної і незалежної держави.

⁴²¹ *Защита персональных данных в сфере телекоммуникационных услуг*: Рекомендации Комитета Министров Совета Европы от 07.02.95, NR(95)4.

⁴²² Закон України «Про інформацію». — Ст. 31.

⁴²³ *Конвенція про захист (прав) фізичних осіб у зв'язку з автоматизованою обробкою персональних даних*. Прийнято Радою Європи 28.01.91.

⁴²⁴ *Защита персональных данных в сфере телекоммуникационных услуг*: Рекомендации Комитета Министров Совета Европы от 07.02.95, NR(95)4.

⁴²⁵ Конституція України. — Ст. 41, 42.

⁴²⁶ Закон України «Про підприємства в Україні» від 27 березня 1991 р. з доп. від 16 грудня 1993 р., №3713-XII // Закони України / Верховна Рада України; Ін-т законодавства. — К.: Книга, 1996. — Т.1. — С 310—331. — Ст.30.

⁴²⁷ Про *перелік* відомостей, що не становлять комерційної таємниці: Постанова Кабінету Міністрів України від 09.08.93, №611. — Машинопис.

⁴²⁸ Закон України «Про охорону прав на винаходи і корисні моделі»; Закон України «Про внесення змін і доповнень до Закону України «Про охорону прав на винаходи і корисні моделі» // Відомості Верховної Ради України. — 2000. — №37.

⁴²⁹ Закон України «Про державну таємницю».

⁴³⁰ Закон України «Про науково-технічну інформацію».

⁴³¹ Закон України «Про охорону прав на винаходи і корисні моделі»; Закон України «Про внесення змін і доповнень до Закону України «Про охорону прав на винаходи і корисні моделі».

⁴³² Закон України «Про державну таємницю».

⁴³³ Закон України «Про інформацію».

ЗМІСТ

<i>Від автора</i>	3
<i>Вступ</i>	9
<i>Розділ 1. КОНЦЕПТУАЛЬНІ ЗАСАДИ ДЕРЖАВНОГО УПРАВЛІННЯ НАЦІОНАЛЬНИМ НАУКОВО-ТЕХНІЧНИМ РЕСУРСОМ</i>	
1.1. Концепт інформаційної політики в сучасному світі.....	35
1.2. Важелі процесу прийняття рішень щодо науково-технологічного розвитку в Україні.....	54
1.3. Інформаційне протиборство і національна безпека у XXI столітті.....	83
1.3.1. Погляди фахівців США на сутність інформаційної війни та інформаційної боротьби.....	83
1.3.1.1 Місце і роль інформаційного протиборства в забезпеченні національних інтересів СІЛА.....	83
1.3.1.2 Роль засобів масової інформації у збройних конфліктах.....	99
1.3.1.3. Погляди військового керівництва США на ведення інформаційної війни.....	103
1.3.2. Інформаційна війна за поглядами військових аналітиків Китаю.....	116
1.3.2.1. Інформаційне протиборство у збройній боротьбі.....	116
1.3.2.2. Значення психологічних операцій в інформаційній війні.....	121
1.3.3. Погляди фахівців Російської Федерації на проблеми інформаційного протиборства.....	126
1.3.3.1. Погляди фахівців Російської Федерації на місце і роль інформаційної боротьби в забезпеченні національних інтересів.....	126
1.3.3.2. Форми і методи забезпечення оборони країни	

і протидії міжнародним силам та іншим країнам в інформаційній боротьбі.....	128
1.3.3.3. Погляди російських військових фахівців на роль інформаційної компоненти у війнах майбутнього.....	129
1.4. Інформація, інформаційна діяльність та її форми на сучасному етапі розбудови державності.....	141
1.4.1. Сутність понять «інформація» та «інформаційні ресурси».....	141
1.4.2. Модель інформаційної сфери.....	148
1.4.3. Інформатизація науки і глобальний інформаційний простір.....	151
1.4.4. Національний інформаційний простір.....	158
1.4.5. Про правовий режим науково-технічної інформації.....	170
1.4.6. Особливості організації змістовного інформаційного ресурсу за науково-технічним доробком як об'єкта державного управління.....	190

Розділ 2. ОРГАНІЗАЦІЙНО-ПРАВОВІ МЕХАНІЗМИ ВІДТВОРЕННЯ НАУКОВОГО ПОТЕНЦІАЛУ В НАЦІОНАЛЬНОМУ ЗМІСЛОВНОМУ ІНФОРМАЦІЙНОМУ РЕСУРСІ

2.1. Інформаційна складова науково-технічної політики держави.....	206
2.1.1. Система охорони інтелектуальної власності.....	221
2.1.2. Науково-технічна інформація та система її організації.....	233
2.1.3. Становлення системи трансферу технологій.....	247
2.2. Право володіння і розпорядження змістовним інформаційним ресурсом за науково-технічним доробком в умовах реструктуризації власності.....	259
2.3. Інформаційний обіг та захист інформації за результатами науково-технічної діяльності у відкритому демократичному суспільстві.....	285
2.3.1. Специфіка використання національного інформаційного ресурсу у відкритому демократичному суспільстві.....	285
2.3.2. Ринкові форми інформаційного обігу та їх правове забезпечення.....	312
2.3.3. Методика і практика віднесення інформації до категорії з обмеженим доступом.....	346

Розділ 3. СТРАТЕГІЯ УПРАВЛІННЯ НАЦІОНАЛЬНИМИ ІНФОРМАЦІЙНИМИ РЕСУРСАМИ ТА ШЛЯХИ ЇЇ ВДОСКОНАЛЕННЯ

3.1. Інституційний характер формування і використання змістовного інформаційного ресурсу з наукового потенціалу України.....	368
--	-----

3.1.1 Інформаційна безпека держави та основні елементи її забезпечення.....	399
Г s~\ S*~Y~~) 3.1.2. Основні елементи системи забезпечення інформаційної *>S безпеки України у сфері науково-технічної діяльності.....	410
3.2. Стратегія управління національними інформаційними ресурсами: модель системної трансформації.....	419
3.3. Організаційні основи вдосконалення системи державного управління інформаційними ресурсами.....	438
Розділ 4. ЗАХИСТ ІНФОРМАЦІЇ — ПРІОРИТЕТНЕ ЗАВДАННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ	
4.1. Історія формування державної системи захисту інформації.....	463
4.2. Проблеми щодо створення правових передумов забезпечення захисту інформаційних ресурсів.....	487
4.2.1. Проблеми у сфері захисту інформаційних ресурсів, віднесених до державної таємниці.....	488
4.2.2. Проблеми у сфері захисту інформації з обмеженим доступом, що не становить державної таємниці.....	511
Висновки.....	530
Примітки.....	539

Наукове видання

СОСНІН Олександр Васильович

ПРОБЛЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ СИСТЕМОЮ
НАЦІОНАЛЬНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ
З НАУКОВОГО ПОТЕНЦІАЛУ
УКРАЇНИ

Монографія

/
ц,^
і)

Г (А

Редактор *О.М.Кузьміна* \ \ / /Л
Художник *О.В.Дендебера* • * \ \ s- ^П /""?
Дизайнер *О.В.Козлітіна* S\ Ls\ ^*

Піди, до друку 18.08.2003, формат 60 * 84/16- Папір офс. № 1. Гарнітура Times.
Офс. друк. Обл.-вид. арк. 35,6. Наклад 500 пр. Вид. № 111/^->y1 (1

Інститут держави і права ім. В.М. Корецького НАН укрेशи/W ^
01001, Київ, вул. Трьохсвятительська, 4 тел. 229-73-96, факс* 228-54*74