Тема IV

ОСНОВНІ НАПРЯМКИ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

§ 1 Класифікація видів інформаційної безпеки

Основні напрямки забезпечення інформаційної безпеки пов'язані з такими суб'єктами, як людина, суспільство, держава. Саме захист їхніх інтересів, прав, свобод щодо правовідносин в інформаційній сфері потребує правого регулювання. Тісний взаємозв'язок і разом з тим специфіка кожного з цих суб'єктів визначається взаємодією заради суспільного блага між державою і громадянським суспільством як суспільством громадян з високим рівнем політичних, культурних, моральних рис. Подібні риси якраз і стають об'єктом захисту в сфері інформаційних правовідносин. І саме щодо них треба визначити існування загроз інформаційним правовідносинам.

Правовий аналіз питань інформаційної безпеки пов'язаний зі значними труднощами насамперед через надмірну політизованість цієї категорії.

Адже конкретний зміст, наповнення категорії інформаційної безпеки, як зазначається в Законі України «Про основи національної безпеки», «обумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам загроз національним інтересам».[1] Таким чином, зміст інформаційної безпеки залежить від політичної позиції тих сил, що стоять при владі в тій чи іншій державі, від змісту теоретичних концепцій, якими вони керуються, тощо. Більше того, неоднозначне розуміння змісту інформаційної безпеки часто існує навіть у національному законодавстві однієї держави.

[1] Закон України «Про основи національної безпеки України» від 19 червня 2003 р. //Голос України. – 22 липня 2003 р. – № 134.

Так, у вищезгаданому законі всі види безпеки, в тому числі й інформаційна, пов'язуються зі станом захищеності життєво важливих інтересів її об'єктів, причому об'єктами називаються:

- людина і громадянин – їхні конституційні права і свободи;
- суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси;
- держава – її конституційний лад, суверенітет, територіальна цілісність і недоторканність.

Одночасно у Концепції національної програми інформатизації, інформаційна безпека називається (п. 3. розділу VI) «невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки». А об'єктами інформаційної безпеки визначаються «інформаційні ресурси, канали інформаційного обміну і телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни»[1].

У сусідній з нами Російській Федерації, яка значно далі просунулася у нормативно-правовому регулюванні питань інформаційної безпеки, існує кілька офіціальних, закріплених у нормативно-правових актах визначень інформаційної безпеки, причому одні для, так би мовити, внутрішнього, а інші – для зовнішнього, міжнародного використання.

Так, у Концепції інформаційної безпеки Російської Федерації, затвердженої Президентом РФ у 2000 р., практично відтворюються в інформаційному контексті положення закону РФ «Про безпеку». І на цій основі визначається, що «під інформаційною безпекою цієї держави розуміється стан захищеності її національних інтересів в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особи, суспільства і держави»[2].

В той же час для сфери зовнішніх зносин пропонується зовсім інше розуміння інформаційної безпеки. Згідно із ст. 2 Федерального закону «Про участь в міжнародному інформаційному обміні», інформаційна безпека трактується як «стан захищеності інформаційного середовища суспільства, який забезпечує її формування, використання і розви-

[1] Закон України «Про Концепцію національної програми інформатизації» від 4 лютого 1998 року № 75/98-ВР

[2] Концепция информационной безопасности РФ. Утверждена Указом Президента РФ от 10 января 2000 г. № 24.// Российская газета. – 2000. – № 24.

ток в інтересах громадян, організацій, держави»[1]. Тобто, знову ж таки, розбіжності виникають навіть у визначенні предмета захисту «інтереси» або «інформаційна сфера».

На нашу думку, найбільш поміркованою виглядає спільна позиція країн-членів Європейського Союзу щодо змісту поняття «інформаційна безпека», яку було висловлено представником Швеції при обговоренні питань міжнародної інформаційної безпеки на 56-й сесії Генеральної Асамблеї ООН:

«Інформаційна та мережна безпека означає захист особистої інформації про відправників і одержувачів, захист інформації від несанкціонованих змін, захист від несанкціонованого доступу до інформації і створення надійного джерела постачання обладнання, послуг та інформації.

Інформаційна безпека також охоплює захист інформації, що стосується військового потенціалу та інших аспектів національної безпеки. Недостатній захист життєво важливих інформаційних ресурсів і інформаційних та телекомунікаційних систем може створити загрозу для міжнародної безпеки»[2].

На нашу думку, така позиція з приводу інформаційної безпеки відзначається насамперед раціоналізмом, адже предметом безпеки називається не аморфна категорія у вигляді «національних інтересів» або «інформаційної сфери», а конкретні поняття різних видів інформації. Крім того, простежується досить чітке розмежування особливостей інформаційної безпеки людини і суспільства (особиста інформація, інформаційне забезпечення життя суспільства) та інформаційної безпеки держави (інформаційне забезпечення національної безпеки).

Слід зазначити, що донедавна (за історичними мірками) головним суб'єктом інформаційної безпеки була держава. Сама проблема інформаційної безпеки держави з'явилася багато століть тому. Існування, наприклад, такого поняття, як державна таємниця, в різних інтерпретаціях простежується ще з найдавніших часів. А згадки про перші засоби шифрування датуються ще 4 тисячоліттям до н.е.[3] З правової точки

---

[1] Федеральный закон РФ «Об участии в международном информационном обмене» от 4 июля 1996 г. № 85-ФЗ. // СЗ РФ. 1996. – № 28. – С. 3347.

[2] «Developments in the field of information and telecommunications in the context of international security». / Report of the Secretary-General. Fifty-six session. 3 July 2001. United Nations. A/56/164.

[3] Див., напр.: Потий О. Криптография, прошлое и настоящее. // Служба безопасности, 2001. – № 2 – 3. – С. 30.

зору важливим також є той факт, що категорії інформаційної безпеки держави формувалися відповідно до волі керівних верств і відповідно ґрунтувалися на пов'язаному з волею держави розвиткові норм *позитивного права*.

В той же час поняття інформаційної безпеки людини та суспільства, умови існування яких визначаються насамперед їхніми природними правами і обов'язками, стає актуальним лише в контексті розвитку і впровадження ідей *природного права*, зокрема прав людини і громадянина[1]. Тобто питання інформаційної безпеки людини почало формуватися не «згори» – від владних органів, а «знизу» – в контексті боротьби за реалізацію інформаційних прав людини, зокрема свободи слова, таємниці приватного життя, прав нації на самовизначення, на національно-культурний розвиток тощо. З цих причин розвиток цього напряму інформаційної безпеки у більшій частині світу припадає на кінець 40-х рр. XX ст., коли були прийняті основні міжнародно-правові акти з прав людини, визнані на міжнародному рівні право націй і народів тощо. А в таких країнах, як Україна або Росія, розвиток напрямків інформаційної безпеки людини і суспільства взагалі бере початок лише в останнє десятиліття XX ст. і пов'язаний з початком демократичних реформ.

Таким чином, саме XX ст. відкрило зовсім нові аспекти інформаційної безпеки, зробивши завдання захисту інформації, яке превалювало до цього, лише одним з її напрямків. Розвиток як природничої, так і гуманітарної сфери науки і виробництва значно змінив акценти і розкрив усю багатоплановість і комплексність поняття «інформаційна безпека». І такий підхід визначає інформаційні процеси нинішнього XXI століття.

Саме на аспекті багатоплановості поняття «інформаційна безпека» наголошує цілий ряд фахівців у галузі інформаційного права, зокрема, підкреслюється, що «інформаційна безпека і, головне, її забезпечення формується як комплексне завдання, яке створює баланс між потребою в інформації великого різноманіття суб'єктів та необхідністю розумно використовувати наявний інформаційний ресурс під девізом «не зашкодь». Такий девіз допомагає розкрити зміст «захисту»: захисту **чого, від чого, в ім'я чого або кого** і, нарешті, **як**. Відповіді на ці

[1] Кормич Б.А. Правові методи попередження та ліквідації загроз інформаційній безпеці людини. // Митна справа. Науково – аналітичний журнал з питань митної справи та зовнішньоекономічної діяльності. – № 5 (вересень – жовтень). – 2002. – С. 75. – 89.

запитання і повинні дати різні концепції, політика інформатизації, законодавство».[1]

Над питанням, що саме являє собою інформаційна безпека, ми вже розмірковували в попередніх розділах, дійшовши висновку, що інформаційна безпека означає наявність певних мінімально необхідних умов існування її суб'єктів, що встановлені міжнародним та національним законодавством. Посилання в цитованому нами визначенні на законодавство як джерело відомостей про конкретний зміст інформаційної безпеки є тому підтвердженням. Адже саме визначеність у законодавстві основних параметрів інформаційної безпеки дозволяє нам розглядати останню як правову категорію.

Повертаючись, до визначеного в розділі I Концепції (основ державної політики) національної безпеки України кола об'єктів інформаційної безпеки: громадянина, суспільства та держави, – слід зазначити, що не всі з них мають чітко визначені законодавством параметри інформаційної безпеки. Так, для громадянина (людини) концепція чітко вказує ці параметри – його права і свободи, і таким чином відсилає нас до міжнародних та національних нормативно-правових актів з прав людини. Так само визначені й основні параметри інформаційної безпеки держави, які охоплюють конституційний лад, суверенітет, територіальну цілісність і недоторканність кордонів, тобто ті категорії, які знову ж таки визначені в національному законодавстві.

А з другого боку, як параметри інформаційної безпеки суспільства концепція називається його (суспільства) духовні та матеріальні цінності. І така постановка питання викликає певні труднощі.

По-перше, така класифікація параметрів інформаційної безпеки здійснена на різних засадах. Адже права і свободи людини або конституційний лад держави є певною системою норм права, а моральні цінності є системою норм моралі, не кажучи вже про матеріальні цінності, які, як правило, є фізичними об'єктами.

По-друге, знову ж таки, законодавством не можуть визначатися загальні, обов'язкові для всіх параметри моральних або матеріальних цінностей. Тобто фактично в даному разі йдеться про невизначені параметри безпеки невизначеного кола осіб.

Наприклад, Конституція України не розглядає окремо інформаційні права суспільства в цілому, крім, мабуть, норм ч. 1 ст. 15 Кон-

[1] Бачило И.Л. Информационное право: основы практической информатики. – М., 2001. – С. 253.

ституції щодо багатоманітності суспільного життя. Але суб'єктами суспільного життя є окремі члени цього суспільства, а не воно саме. Таким чином, для визначення параметрів інформаційної безпеки суспільства необхідно пов'язати його із визначеними параметрами інформаційної безпеки окремих його членів. І це не дивно, адже, виходячи з більшості сучасних правових доктрин в галузі прав людини, ми можемо стверджувати, що права групи осіб або суспільства в цілому визначаються сукупністю особистих прав його членів. Як зазначає, наприклад, П.М. Рабинович, «...одним з неодмінних складників загальносоціальних прав людини є можливість зберігати, виявляти, реалізовувати й розвивати свою національну самобутність. Тому забезпечення даного права кожному члену певної національної спільноти є водночас і забезпеченням відповідних етнічних прав всієї цієї групи людей. І навпаки: забезпечення прав нації в цілому дає змогу, ясна річ, кожному її представникові реалізовувати свої етнічні права»[1]. Звісно, таке твердження не ототожнює права нації та права людини, але розкриває їхній діалектичний взаємозв'язок.

З другого боку, якщо повернутися до цілого ряду фундаментальних актів в галузі прав людини, то права нації в них розглядаються в певному контексті.

Так, наприклад, правам нації присвячено частину І Міжнародного пакту про громадянські і політичні права[2] та частину І Міжнародного пакту про економічні, соціальні і культурні права[3], причому відповідні права нації викладено абсолютно ідентично. Основним правом народу (нації) згідно з ч. 1 ст. 1 Міжнародного пакту про громадянські і політичні права є право на самовизначення. Підкреслюється, що саме на підставі цього права народи вільно встановлюють свій політичний статус і вільно забезпечують свій економічний, соціальний і культурний розвиток.

Норми ч. 2. ст. 1 Міжнародного пакту про громадянські і політичні права вже визначають *засоби реалізації* вищевизначених прав народу. Так, підкреслюється, що «всі народи для досягнення своїх цілей можуть вільно розпоряджатися своїми природними багатствами і ресурсами без шко-

[1] Рабинович П.М. Основи загальної теорії права та держави. – К.: Атака, 2001. – С. 20 –21.

[2] Міжнародний пакт про громадянські і політичні права. Прийнято 16 грудня 1966 року Генеральною Асамблеєю ООН. Док. ООН A/RES/2200 A (XXI)

[3] Міжнародний пакт про економічні, соціальні і культурні права. Прийнято 16 грудня 1966 року Генеральною Асамблеєю ООН. Док. ООН A/RES/2200 A (XXI)

ди для будь-яких зобов'язань, що випливають з міжнародного економічного співробітництва, заснованого на принципі взаємної вигоди, та з міжнародного права. Жоден народ ні в якому разі не може бути позбавлений належних йому засобів існування». Таким чином, нормами ч. 2 ст. 1 Міжнародного пакту про громадянські і політичні права фактично підкреслюється, що народ (суспільство) в цілому також має право на певні *колективні умови існування*, які поширюються на всіх представників цього народу, і є чимось самобутнім. Але ця загальна самобутність суспільства, цілком природно, визначається самобутністю кожного з членів цього суспільства. І на практиці самовизначення нації, обрання нею певних умов свого існування залежить від волі більшості її представників. Адже «права людини (права особи) розглядаються в сучасному міжнародному праві як права якщо не пріоритетні, то щонайменше рівні правам нації (народу). Але права нації (народу), зокрема право на самовизначення, суть лише *колективні права людини*... Відповідно, замахи на право нації (народу) на самовизначення – це *масові порушення прав людини*»[1] . Таким чином, якщо замахом на інформаційну безпеку людини ми можемо вважати насамперед порушення прав і свобод людини в сфері інформації, якими і визначається стан інформаційної безпеки людини, то замахом на інформаційну безпеку суспільства можна вважати такі порушення інформаційних прав і свобод людини, які носять масовий характер і негативно впливають на рівень інформаційної безпеки значної кількості членів цього суспільства.

Також в аспекті питання інформаційної безпеки суспільства важливою для нас є норма ч. 3 ст.1 Міжнародного пакту про громадянські і політичні права, згідно з якою «всі держави... повинні, відповідно до положень Статуту Організації Об'єднаних Націй, заохочувати здійснення права на самовизначення і поважати це право». Таким чином, саме держава визначається тим інструментом або механізмом, за допомогою і через який реалізовуються права народу (нації), досягаються його цілі. Але, звісно, лише та держава, яка є демократичною і в якій забезпечується дотримання прав і свобод людини, в тому числі і в сфері інформації.

З огляду на вищесказане, ми можемо говорити про те, що інформаційна безпека суспільства може розглядатися *лише в комплексі* з інформаційною безпекою людини.

---

[1] Тарасов А. Право народов на самоопределение как фундаментальный демократический принцип.// Свободная Мысль. Теоретический и политический журнал, 2002. – № 9. – С. 66.

Цей комплексний характер інформаційної безпеки людини та суспільства визначається цілим рядом елементів, в тому числі рядом базових, до яких належать:

- права і свободи людини і громадянина в сфері інформації;
- державні механізми забезпечення та реалізації інформаційних прав і свобод людини та права нації на самовизначення (політичне, культурне, економічне);
- демократичний механізм формування політичної влади в державі, який дає можливість окремій людині та суспільству в цілому через механізми народовладдя визначати основні параметри інформаційних процесів у державі.

В той же час на державу покладено обов'язки забезпечення відповідних прав і людини, і народу в цілому. Так, ч. 2 ст. 3 Конституції України визначає, що «утвердження і забезпечення прав і свобод людини є головним обов'язком держави», а ст. 11 Конституції України визначає, що «держава сприяє консолідації і розвиткові української нації, її історичної свідомості, традицій, культури, а також розвиткові етнічної, культурної, мовної та релігійної самобутності всіх корінних народів і національних меншин України». Що, в свою чергу, доповнюється функцією держави щодо захисту інформаційної безпеки (ч. 1. ст. 17 Конституції України)[1].

Таким чином, до сфери інформаційної безпеки держави входять конкретні дії щодо забезпечення безпечних умов існуючих інформаційних процесів та забезпечення безпечного розвитку таких процесів у майбутньому. Це охоплює регулювання питань захисту самої інформації, захисту інформаційної інфраструктури держави, захисту інформаційного ринку та створення безпечних умов розвитку інформаційних процесів. Все це досягається проведенням необхідної державної політики інформаційної безпеки та створенням необхідних правових та організаційних засад.

Така конструкція вказує насамперед на головну роль держави у забезпеченні інформаційної безпеки всього кола об'єктів (людини, суспільства і самої держави) і, з другого боку, пояснює, чому в тому ж законодавстві США (країни, де вперше було застосовано термін «національна безпека») інформаційну безпеку пов'язують насамперед із певними аспектами державної діяльності[2].

---

[1] Конституція України. Прийнята Верховною Радою України 28 червня 1996 року // Відомості Верховної Ради України, 1996. – №30 – Ст. 141.

[2] Див., напр.: Ex. Ord. No. 12958. Classified National Security Information (Source Ex. Ord. No. 12958, Apr. 17, 1995, 60 F.R. 19825, as amended by Ex. Ord. No. 12972, Sept. 18, 1995, 60 F.R. 48863; Ex. Ord. No. 13142, Nov. 19, 1999, 64 F.R. 66089)

Аналізуючи класифікацію об'єктів та предметів різних аспектів інформаційної безпеки, необхідно відзначити одну особливість, властиву цілому ряду пострадянських країн, в тому числі й України. Це певна захопленість створенням різного роду концепцій. Ми вже наводили приклади того, що для американського та західноєвропейського підходу до питань інформаційної безпеки властиві насамперед прагматизм та зосередженість на об'єктах і цілях (бачанні перспективи) політики інформаційної безпеки, чіткому прописуванні всіх її елементів. В той же час для концепцій інформаційної безпеки країн СНД, які створювалися під впливом передусім відповідних ідей і концепцій Російської Федерації, головною особливістю є те, що вони будуються не на об'єктно-цільовій базі, а на базі «загроз та інтересів»[1]. Покладення в основу концепції інформаційної безпеки означеної системи «загроз та інтересів», на нашу думку, веде до недієздатності самої концепції. Адже такі категорії, як «загрози» та «інтереси», є надто аморфними і суб'єктивними для того, щоб їх викладати лаконічною і формалізованою мовою нормативно-правових актів. Насичення нормативно-правового акту нормами-деклараціями означає фактичну відсутність у нього будь-якої регулятивної сили. А це, в свою чергу, порушує самі основи побудови законодавства, приводить до появи недосконалих нормативно-правових актів, в яких відсутні механізми їх юридичної дії, створює прогалини, колізії у правовому регулюванні питань інформаційної безпеки.

Так, наприклад, Концепція (основи державної політики) національної безпеки України 1997 року в розділі III називає такі основні загрози національній безпеці України в інформаційній сфері:

- невиваженість державної політики та відсутність необхідної інфраструктури в інформаційній сфері;
- повільність входження України у світовий інформаційний простір, брак у міжнародного співтовариства об'єктивного уявлення про Україну;
- інформаційна експансія з боку інших держав;
- витік інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави;
- запровадження цензури.[2]

---

[1] Див.: Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право. / Под. ред. акад. РАН Б.Н. Топорнина. – СПб.: Юридический центр Пресс», 2001. – С. 421 – 458.

[2] Постанова Верховної Ради України «Про концепцію (основи державної політики) національної безпеки України» від 16 січня 1997 р. № 3/97-ВР // Голос України, 1997. – 4 лютого – С. 5

Схожа класифікація міститься і у Законі України «Про основи національної безпеки» (ст. 7), де серед загроз національній безпеці України в інформаційній сфері називаються:

- прояви обмеження свободи слова та доступу громадян до інформації;
- поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- комп'ютерна злочинність та комп'ютерний тероризм;
- розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;
- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.[1]

Цікавим елементом аналізу вищезазначених загроз інформаційній безпеці є визначення суб'єкта цих загроз, тобто суб'єкта, чиїми діями або бездіяльністю такі загрози можуть створюватися. Безпосередньо в концепції називається лише суб'єкт інформаційної експансії – інші держави. А ось щодо інших загроз, то постає така картина. Суб'єктом державної політики, невиваженість якої називається загрозою, є, безумовно, Українська держава, так само до функцій держави, згідно із законами «Про інформацію»[2] та «Про національну програму інформатизації»[3], належать створення інформаційної інфраструктури, входження у світовій інформаційних простір тощо. Цензура, як правило, також запроваджується державою та її органами. Таким чином, згідно з концепцією більшість основних загроз інформаційній безпеці походить від діяльності органів публічної влади Української держави.

Але чи правильно було б називати подібні загрози загрозами інформаційній безпеці? Коли ми говоримо, що система публічної влади має певні вади, які вкрай негативно впливають на умови існування цієї системи, мова повинна йти саме про недоліки або недостатню ефективність самої системи, а не про загрозу її безпеці. Наприклад, на нашу думку, невиваженість інформаційної політики держави або відсутність

[1] Закон України «Про основи національної безпеки України» від 19 червня 2003 р. //Голос України. – 22 липня 2003 р. – № 134.

[2] Закон України «Про інформацію» від 2 жовтня 1992 р. // Відомості Верховної Ради України, 1992. – № 48. – С. 650.

[3] Закон України «Про Концепцію національної програми інформатизації» від 4 лютого 1998 року № 75/98-ВР

необхідної інформаційної інфраструктури безпосередньо не містять у собі загрози, але ці фактори знижують потенціал держави, необхідний для захисту інформаційної безпеки. Таким чином, треба розмежовувати безпосередні загрози інформаційній безпеці та засоби забезпечення цієї безпеки, які спрацьовують лише при виникненні загрози.

На жаль, починаючи від створення Концепції національної безпеки, закладені в ній аморфні і нечіткі формулювання «загроз», значна частина яких скоріше належить до недоліків інституціональних та правових механізмів, автоматично поширилися у багатьох розробках у галузі інформаційної безпеки.

Так, наприклад, свого часу в науковій доповіді Національного інституту стратегічних досліджень було визначено такі загрози інформаційній безпеці:

- Слабка інтегрованість України у світове інформаційне поле, недостатня кваліфікація й активність її інформаційних служб.
- Використання засобів інформації окремими політичними силами.
- Негативні наслідки міжпартійних відносин.
- Вплив міжконфесійних конфліктів.
- Некомпетентність працівників державних органів і установ.
- Недостатній професійний рівень працівників засобів масової інформації.
- Вплив на засоби масової інформації організованої злочинності, мафіозних структур.
- Недостатність технічного захисту інформаційного простору України.[1]

Певні позитивні кроки щодо виявлення та окреслення загроз інформаційній безпеці України ми можемо побачити в аналітичних розробках Українського центру економічних і політичних досліджень ім. О. Розумкова. Так, зокрема, експерти цього центру пішли шляхом виділення окремо факторів, що становлять загрозу інформаційній безпеці, та чинників ескалації цих загроз. Така конструкція виглядає цілком слушною, оскільки названі її елементи мають різну природу і різні механізми впливу на стан інформаційної безпеки України.

Так, підкреслюється, що негативні тенденції розвитку інформаційного простору України, недосконалість системи забезпечення

[1] Див.: Національна безпека України, 1994 – 1996 рр. Наукова доповідь НІДС. / Редкол.: О.Ф. Бєлов (голова) та ін. – К.: НІДС, 1997. С. 124 – 125.

інформаційної безпеки, кризовий стан вітчизняної економіки створюють передумови для ескалації загроз інформаційній безпеці України.

Чинники, що зумовлюють ескалацію загроз інформаційній безпеці, мають комплексний характер – вони охоплюють усі сфери життєдіяльності людини, суспільства і держави.[1]

Іншими словами, пропонується окремо розглядати стан та параметри існування держави, суспільства, окремих громадян, відповідних державних, громадських і приватних інституцій у сфері інформаційних відносин і визначати ті їх елементи, які є «слабким ланцюгом» у разі виникнення загроз.

Однак, попри таку прогресивну точку зору, ми знову бачимо досить стандартний підхід до визначення наявних і потенційних загроз інформаційній безпеці. Зміст цього підходу полягає в безпосередньому аналізі сучасного становища інформаційної сфери в Україні і на його базі створенні певного експертного передбачення всіх можливих загроз інформаційній безпеці. Саме за допомогою таких методів було сформульовано наступний перелік загроз, серед яких:

- обмеження свободи слова та доступу громадян до інформації;
- руйнування системи цінностей, духовного та фізичного здоров'я особи, суспільства, негативні зміни їх цільових настанов;
- маніпулювання громадською думкою з боку державної влади, фінансово-політичних кіл;
- обмеження можливостей органів державної влади приймати адекватні рішення;
- порушення штатного режиму функціонування (руйнування) критично важливих інформаційних мереж, систем управління;
- несанкціонований витік таємної, конфіденційної та іншої інформації з обмеженим доступом;
- спотворення, знищення інформаційних ресурсів, програмного забезпечення;
- низький рівень інтегрованості України у світовий інформаційний простір.[2]

На нашу думку, цінність такого підходу є досить сумнівною. Так, ми можемо говорити, що ситуація в Україні і світі постійно змінюється, що саме діалектичний підхід до аналізу цих змін є найбільш ефек-

[1] Чинники ескалації загроз інформаційній безпеці України. // Національна безпека і оборона, 2001. – № 1. – С. 29.

[2] Концепція (основи державної політики) інформаційної безпеки України. Проект УЦЕПД // Національна безпека і оборона, 2001. – № 1. – С. 53.

тивним. Але така методологія більшою мірою підходить для визначення конкретних цілей і політики держави на конкретно-історичному етапі розвитку.

§ 2 Принципи правового регулювання напрямків інформаційної безпеки

На відміну від різного роду концепцій і теоретичних розробок, *правове регулювання вимагає однозначності та стабільності правових норм*. Тому вищезгадані принципи побудови офіційної, юридично закріпленої концепції інформаційної безпеки на основі так званої «теорії загроз» не є ефективними з точки зору правового регулювання відповідних суспільних відносин.

У зв'язку з цим не можна не відзначити значний крок щодо вдосконалення правового регулювання питань інформаційної безпеки, який було зроблено авторами Концепції інформаційної безпеки Російської Федерації, яку було прийнято указом Президента РФ у 2000 р. Попри збереження концептуального підходу на основі згаданої системи «загроз та інтересів», сама концепція будується не на переліку загроз національним інтересам, а на *класифікації видів загроз*. Тобто загрози інформаційній безпеці формулюються залежно від інтересів, потреб та цілей конкретних об'єктів, проти яких ці загрози спрямовані, що означає спробу поєднання в одному нормативно-правовому акті досвіду «заходу» і «сходу» у вигляді концепції «об'єктів та цілей» і концепції «загроз та інтересів». І це дало, на нашу думку, потрібний результат.

Так, згідно з п. 2 розділу I Концепції інформаційної безпеки РФ, за своєю загальною спрямованістю загрози інформаційній безпеці РФ підрозділяються на такі види:

- загрози конституційним правам і свободам людини та громадянина у сфері духовного життя й інформаційної діяльності, індивідуальній, груповій і суспільній свідомості, духовному відродженню держави;
- загрози інформаційному забезпечення державної політики;
- загрози розвиткові вітчизняної індустрії інформації, включаючи індустрію засобів інформатизації, телекомунікації і зв'язку, забезпеченню потреб внутрішнього ринку в її продукції і виходу цієї продукції на світовий ринок, а також забезпеченню накопичення, збереження й ефективного використання вітчизняних інформаційних ресурсів;

• загрози безпеці інформаційних та телекомунікаційних засобів і систем, як вже розгорнутих, так і тих, що створюються на території держави[1].

Неважко помітити, що наведена класифікація видів загроз має досить мало спільного з концепцією національних інтересів в інформаційній сфері. Тут перераховують певні явища або об'єкти, руйнування яких може призвести до негативних наслідків здійснення інформаційних процесів в державі. Більше того, викладені в першому пункті об'єкти загроз визначають параметри інформаційної безпеки насамперед людини і суспільства. В той же час у решті пунктів мова йде про ті об'єкти, якими визначається рівень інформаційної безпеки держави і її здатність забезпечувати інформаційну безпеку своїх громадян.

Крім того, потрібно відзначити наявність у Концепції інформаційної безпеки РФ розділу II «Методи забезпечення інформаційної безпеки Російської Федерації», в якому визначені основні напрямки державної діяльності у внутрішньо- та зовнішньополітичній сферах і способи її здійснення задля досягнення конкретних цілей в галузі інформаційної безпеки. Це є тим аспектом, якого явно не вистачає у більшості вітчизняних концепцій інформаційної безпеки, і до того ж свідчить, що автори цього документа спробували відійти від традиційного російського популізму і звернутися до західного раціоналізму.

Проаналізований матеріал дає можливість запропонувати ряд принципів побудови концепції інформаційної безпеки, які забезпечили б досконалість нормативно-правового регулювання.

По-перше, ми наполягаємо на принциповому розмежуванні інформаційної безпеки людини і суспільства та інформаційної безпеки держави. Таке розмежування обумовлюється не лише різницею завдань, що вирішуються для забезпечення безпеки цих суб'єктів. Головним чинником є різна природа норм права, що визначають основні параметри безпеки цих суб'єктів. Інформаційна безпека людини та суспільства ґрунтується на нормах природного права, якими визначаються невід'ємні права і свободи людини та громадянина, в той же час параметри інформаційної безпеки держави ґрунтуються на нормах позитивного права, які самою державою і встановлюються.

Світовою тенденцією є уніфікація захисту прав і свобод людини, їх єдино образне тлумачення і реалізація, на що спрямована велика

[1] Концепция информационной безопасности РФ. Утверждена Указом Президента РФ от 10 января 2000 г. № 24.// Российская газета. – 2000. – № 24.

кількість міжнародно-правових актів, учасником яких є і Україна. В той же час параметри інформаційної безпеки держави є абсолютно індивідуальними для кожної держави, і вимог щодо їх уніфікації не ставиться. Таким чином, розглядаючи проблеми інформаційної безпеки людини і суспільства та проблеми інформаційної безпеки держави, ми повинні усвідомлювати, що маємо справу з двома абсолютно різними за своєю природою явищами.

По-друге, захист інформаційної безпеки є однією з функцій держави, тобто певною константою, яка наповнюється конкретним змістом залежно від обставин.

По-третє, національне законодавство повинно визначати ті мінімально необхідні умови і параметри інформаційних процесів, які можуть вважатися безпечними для існування людини, суспільства і держави.

Таким чином, будь-яка класифікація загроз інформаційній безпеці повинна ґрунтуватися не лише на аналізі об'єктивних факторів існування держави, а й на аналізі певного масиву правових норм, на основі яких ми можемо об'єктивно визначити, що є безпечним, а що становить загрозу.

Взагалі, аналізуючи проблему загроз інформаційній безпеці, потрібно від самого початку визначитись, що саме може розцінюватись як загроза. На нашу думку, по-перше, загрозу можуть нести лише певні дії (діяльність або бездіяльність), які мають прямий причинно-наслідковий зв'язок зі зміною відповідних умов і параметрів інформаційних процесів, що визначають безпечні умови існування суспільства і держави.

По-друге, ці дії повинні бути конкретно визначеними, а не загальними. Тобто, якщо ми розцінюємо певні дії як загрозу інформаційній безпеці, ми повинні мати відповіді на питання, хто скоїв ці дії, що саме він скоїв і коли.

І, по-третє, ще одним фактором повинен бути рівень суспільної небезпеки цих дій. Наприклад, коли визначається, що загрозу інформаційній безпеці становлять «спотворення, знищення інформаційних ресурсів, програмного забезпечення», це є дуже загальним формулюванням. Адже проникнення або знищення бази даних органів внутрішніх справ і такі самі дії стосовно інтернет-сторінки популярного співака або футбольного клубу мають зовсім різний ступінь суспільної небезпеки та різні наслідки для рівня інформаційної безпеки України.

Безумовно, що дії, які можуть розцінюватися як загроза інформаційній безпеці, повинні мати виключно високу суспільну небезпеку, адже їх об'єктом є не просто права чи законні інтереси певних суб'єктів, а правові відносини щодо забезпечення умов, порушення яких ставить під сумнів саму можливість нормального існування цих суб'єктів.

Ми кажемо «безумовно», тому що національним законодавством вже було сприйнято подібну ідею і створено певну нормативно-правову основу для аналізу і визначення видів і характеру дій, що можуть бути визначено як загроза інформаційній безпеці.

Зокрема, у новий Кримінальний кодекс України[1] першим в особливій частині було включено розділ «Злочини проти основ національної безпеки України». Зібрані в цьому розділі злочини становлять високу суспільну небезпеку і до їх числа віднесено: дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади (ст. 109); посягання на територіальну цілісність і недоторканність України (ст. 110); державна зрада (ст. 111); посягання на життя державного чи громадського діяча (ст. 112); диверсія (ст. 113) та шпигунство (ст. 114).

Ряд з перерахованих складів злочинів проти основ національної безпеки може завдати шкоди інформаційній безпеці України.

Так, ч. 2 ст. 109 КК визнає злочином «публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій». А ч. 3 ст. 109 КК визначає як більш тяжкий злочин «дії, передбачені частиною другою цієї статті, вчинені особою, яка є представником влади, або повторно, або організованою групою, або з використанням засобів масової інформації».

Згідно з нормами ч. 1. ст. 110 КК визнаються злочинними публічні заклики чи поширення матеріалів із закликами до вчинення умисних дій з метою зміни меж території або державного кордону України на порушення порядку, встановленого Конституцією України. Більш небезпечними визнаються названі дії, якщо вони «вчинені особою, яка є представником влади, або повторно, або за попередньою змовою групою осіб, або поєднані з розпалюванням національної чи релігійної ворожнечі» (ч. 2 ст. 110 КК), або якщо такі дії «призвели до загибелі людей або інших тяжких наслідків» (ч. 3 ст. 110 КК).

---

[1] Кримінальний кодекс України. Прийнятий сьомою сесією Верховної Ради України 5 квітня 2001 р. – Київ: Юрінком-Інтер, 2001.

Один із складів такого злочину, як державна зрада (ст. 111 КК), зокрема, також включає «діяння, умисно вчинене громадянином України на шкоду... інформаційній безпеці України: перехід на бік ворога в умовах воєнного стану або в період збройного конфлікту, надання іноземній державі, іноземній організації або їх представникам допомоги в проведенні підривної діяльності проти України».

Загрозу інформаційній безпеці може становити також диверсія (ст. 112 КК), склад якої включає «вчинення з метою ослаблення держави вибухів, підпалів або інших дій, спрямованих на... руйнування або пошкодження об'єктів, які мають важливе народногосподарське чи оборонне значення». Це стосується і об'єктів інформаційної інфраструктури, які можуть бути предметом злочинного посягання.

І, нарешті, виключно «інформаційний» злочин проти національної безпеки – шпигунство (ст. 113 КК), який визначається як «передача або збирання з метою передачі іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю, якщо ці дії вчинені іноземцем або особою без громадянства».

Показовим є також те, що передбачається звільнення від кримінальної відповідальності за державну зраду та шпигунство в тих випадках, якщо ніяких дій, що шкодять національній безпеці, не було вчинено, або такі дії було добровільно припинено і повідомлено компетентні державні органи про отримані завдання. Тобто ще раз підкреслюється принцип виключної суспільної шкоди і небезпеки для кваліфікації подібних дій.

Звісно, неможливо обмежувати перелік дій, що становлять загрозу інформаційній безпеці, лише тими, за які передбачена кримінальна відповідальність, як за посягання на основи національної безпеки. Особливо з позиції тих, хто звик довільно використовувати цю риторику. Але разом з тим потрібно говорити про фактор юридичної відповідальності і виключної суспільної небезпеки як про обов'язкові ознаки щодо кваліфікації дій як таких, що становлять загрозу інформаційній безпеці України. І про необхідність максимального скорочення і деталізації загроз згідно з означеними нами характеристиками. Вести мову про загрозу національній безпеці можна лише у випадках, чітко визначених законодавством, а не на основі якихось там аналізів та досліджень.

Отже, замахом на інформаційну безпеку є лише ті дії, за які законом передбачено відповідальність. Не передбачено відповідальності – немає і загрози, немає і замаху. Така принципова позиція покладе край

різного роду спекуляціям і утискам свободи слова та інформаційних прав і свобод людини з боку держави та її органів під прапором захисту інформаційної безпеки. І, на нашу думку, переходити на ці позиції треба якнайшвидше. Адже існуючі в Україні сьогодні «офіційні» і «напівофіційні» теорії національної безпеки являють собою не що інше, як інструмент придушення свободи слова і політичної боротьби сил, що перебувають при владі. Вже проявляється не те що ухил, а цілеспрямований рух України до рівня різного роду «бананових республік», тоталітарні режими яких широко користуються «індульгенцією» захисту національних інтересів і національної безпеки для виправдання своїх протиправних дій.

Останнім часом світова спільнота приділяє дуже багато уваги тому, що «країни з недемократичними режимами вже дали чимало прикладів переслідування преси під гаслом захисту національних інтересів і національної безпеки...

Педалювання владою необхідності захисту національних інтересів, а потому і контролю діяльності мас-медіа часто супроводжуються сентенціями, які не лише не викликають настороги у пересічного громадянина, а й можуть викликати певну підтримку через уявну «користь» такого контролю заради національних інтересів...

З такими формулюваннями про захист національних інтересів і національної безпеки обмежена свобода мас-медіа у Білорусі (указ Кабінету Міністрів від 18 березня 1997 р.), у Китаї (закон про пресу від лютого 1997 р. забороняє публікацію матеріалів, які шкодять національній безпеці), в Малайзії (акт внутрішньої безпеки), в Пакистані (антитерористичний акт), у Сінгапурі та Південній Кореї (закон про національну безпеку), Алжирі (міжміністерський указ від березня 1994 р. забороняє публікувати матеріали з проблем безпеки, якщо ці матеріали не походять із державного інформагентства), Іран (закон про пресу забороняє публікації матеріалів, які «шкодять національній безпеці»)».[1]

Знову ж таки характерним є те, що, наприклад, комп'ютерні злочини винесено в окремий розділ Кримінального кодексу і безпосередньо з проблемами національної безпеки вони не пов'язуються. І це має певний сенс, оскільки, на нашу думку, не кожна протиправна дія щодо інформації або інформаційних процесів становить загрозу інфор-

[1] Слісаренко І.Ю, Практичне втілення «свободи слова» на пострадянському просторі. – Національний демократичний інститут міжнародних відносин. – К., 2002. – С. 2 – 3.

маційній безпеці, як це інколи хотілося б представити. Адже нормативно-правова основа інформаційної безпеки є лише однією зі складових нової галузі інформаційного права.[1]

Крім того, ще одним фактом є те, що правові норми, які регулюють проблеми інформаційної безпеки, є найбільш давньою і сталою частиною інформаційного права. І не зважати на це є великою помилкою. Адже останнім часом, коли йдеться про інформаційну безпеку, найчастіше доводиться чути про комп'ютерні технології, про злочини за допомогою Інтернет тощо. Разом з тим забувають, що безпосереднім предметом правових відносин у сфері інформаційної безпеки є сама інформація, а не її носії. І загроза вимірюється змістом і характеристиками цієї інформації, а не характеристиками її носіїв. І в цьому сенсі проблема інформаційної безпеки не змінюється. Змінюються лише способи та методи вчинення як дій, що містять загрозу, так і заходів щодо нейтралізації цих загроз.

Таке твердження яскраво ілюструється запропонованим не так давно М. Кранцбергом законом відносин між технологією і суспільством: «Перший закон Кранцберга наголошує: технологія ні гарна, ні погана і ні нейтральна»[2]. Це означає, що будь-яка технологія не несе початково ані негативного, ані позитивного впливу, наслідки залежать передусім від мети її застосування. А ця мета обумовлюється людською природою. В цьому аспекті, наприклад, середньовічні шпигуни нічим не відрізнялися від сучасних. Або загальна мета пропаганди 30-40-х рр. не відрізнялася від сучасної. Інша річ, що застосовуються нові способи і методи вирішення старих завдань. І це призводить до того, що технологія, змінюючи та розширюючи можливості, деякою мірою змінює і свідомість людини, яка є сучасником цієї технології.

Складний механізм впливу інформаційних технологій на суспільство підкреслює і відомий теоретик інформаційного суспільства М. Кастельс. Зокрема, він наголошує на «всеосяжності ефектів нових технологій. Оскільки інформація є інтегральною частиною всякої людської діяльності, всі процеси нашого індивідуального і колективного існування безпосередньо формуються (хоча, безумовно, не детермінуються) новим технологічним способом».[3]

---

[1] Див., напр., Копылов В.А. Информационное право. – М.: Юристъ. – 1997. – С. 26 –29.

[2] Kranzberg, M. The informational age: evolution or revolution? In Bruce R. Guile (ed.), Information Technologies and Social Transformation, Washington D.C.: National Academy of Engineering. – 1985. – p. 50

[3] Кастельс М. Информационная эпоха: экономика, общество, культура: Пер. с англ. под науч. ред. Шкаратана О.И. – М.: ГУ ВШЭ, 2000. – С.77.

Ми маємо справу зі стабільними об'єктами інформаційної безпеки, але одночасно зі змістом та способами захисту, які швидко змінюються. Інформація та інформаційні технології створюються і змінюються людством і одночасно змінюють саме людство. Інформаційні технології є окремим напрямком людської діяльності і одночасно проникають в усі сфери цієї діяльності. Цей дуалізм інформаційної безпеки, її внутрішня діалектика перетворюють її на одну з найбільш складних та динамічних проблем національної безпеки взагалі.

Наприклад, кілька років тому за результатами слухань у Конгресі США було погоджено, що «кінець «холодної війни» та величезне зростання використання інформаційних технологій змінили довкілля, в якому розвідувальні системи повинні діяти. В той же час розвідувальні системи зазнавали значних змін у відповідь на динаміку розвитку в стратегічних і бюджетних питаннях. Придбання і утримання супутникових систем є ключовим для забезпечення вчасної розвідувальної інформації національним політикам та досягнення інформаційної переваги для військового керівництва»[1].

Але традиційні підходи до інформаційної безпеки вже не виглядають єдино правильними у так званому світі «після 11 вересня 2001 р.». Вся система отримання стратегічної інформації США виявилася нездатною попередити найбільшу у світі терористичну атаку. З огляду на це, дедалі більше дослідників доходить висновку, що національна безпека окремої країни, побудована на принципах закритих систем, стає неефективною. Національні системи безпеки побудовані передусім на принципах конкуренції, а не співробітництва і стають беззахисними перед новими викликами. Зміст цих викликів як у матеріальній, так і в духовній сферах обумовлюється цілим рядом факторів.

«У матеріальній сфері помітно розширилися виробничі, творчі можливості... посилилися контрасти бідності та багатства, зросли руйнівні тенденції. Сучасні технічні і технологічні досягнення підготували дешеві асиметричні, але достатньо ефективні засоби протидії традиційним методам завоювання військово-політичного володарювання. Величезні армії і дороге озброєння виявилися безпорадними перед застосуванням цивільних технологічних досягнень, біоматеріалів як фізичних і психологічних факторів масового ураження населення. Терористичні акти в США показали світовій спільноті цю нову зброю і

[1] National Commission For The Review Of The National Reconnaissance Office. Pub. L. 106-120, title VII, Dec. 3, 1999, 113 Stat. 1620, Sec. 701. Findings.

тактику її застосування. Є всі підстави вважати, що форми та межі латентної зброї далеко не вичерпані. Більше того, вони будуть поширюватися разом з визріванням нових високих технологій.

Другий зсув, що змінив уявлення про безпеку, відбувся у духовній сфері суспільства. Кількісно зростаюче бідне населення на землі рано чи пізно повинно було ідеологічно та інституційно оформити свої інтереси... Відмова багатих країн «ділитися» з бідними, з одного боку, підготувала соціальний і політичний ґрунт для зловісного явища сучасного тероризму, а з другого – ще раз зі всією гостротою поставила питання про стабілізацію та сталість суспільного буття як такого. Вийшовши з періоду «холодної війни», світова цивілізація без зволікань увійшла в період катастроф, що продукуються перш за все соціальною і політичною невлаштованістю глобального суспільства, яке народжується».[1]

Розуміння цих факторів створює засади теоретичного і практичного обґрунтування так званої системи глобальної соціальної безпеки, системи, побудованої не на закритості і конфронтації, а на відкритості і широкому співробітництві. Ця проблема є надзвичайно актуальною для сфери інформаційної безпеки. Адже будь-які терористичні акти спрямовані саме на залякування і створення відчуття небезпеки, невпевненості широких верств суспільства. Разом з тим нові виклики актуалізують і іншу небезпеку, про яку ми вже писали, – це небезпека масової істерії і безумовної підтримки будь-яких дій уряду, начебто спрямованих на підтримання безпеки. Цей другий аспект призведе не до підвищення рівня безпеки, а до створення поліцейської або військової держави, яка, нехтуючи правами людини, обмежуючи ці права, являє собою чинник небезпеки.

Ось чому коло проблем, що вирішуються в рамках інформаційної безпеки, потребує чіткого визначення й окреслення.

З огляду на окреслені проблеми досить цікавим є те, що погляди на характер загроз інформаційній безпеці працівників відповідних спецслужб значно відрізняються від цитованих нами політико-правових концепцій. Зокрема, найбільш актуальними загрозами інформаційній безпеці в 2001 р. визначалися такі:

- руйнування національного інформаційного простору або його використання в антидержавних інтересах;
- нав'язування особі, суспільству (шляхом інформаційних впливів на свідомість, підсвідомість, інформаційні ресурси та соціо-технічні

[1] Левашов В.К. Глобализация и социальная безопасность. // СОЦИС, 2002. – № 3. – С. 25.

системи) бажаних для іншої сторони рішень у життєво важливих сферах суспільної і державної діяльності;

• використання засобів масової інформації з позицій, що суперечать інтересам громадян, організацій і держави, маніпулювання інформацією (дезінформація, приховування або спотворення інформації);

• порушення встановленого порядку інформаційного обміну, несанкціонований доступ або необґрунтоване обмеження доступу до інформаційних ресурсів, протиправний збір і використання інформації;

• витік інформації, що містить державну та іншу, передбачену законом таємницю, а також конфіденційну інформацію, яка є власністю держави;

• розв'язування інформаційного протиборства (розповсюдження комп'ютерних «вірусів», встановлення програмних і апаратних закладних пристроїв, впровадження радіоелектронних приладів перехоплення інформації в технічних засобах і приміщеннях, перехоплення і дешифрування інформації, радіоелектронний вплив на парольно-ключові системи, радіоелектронне придушення ліній зв'язку і систем керування та ін.)[1]

У даному разі ми бачимо абсолютно реалістичний погляд на проблему інформаційної безпеки, який можна було б поставити як взірець, якщо тільки у фразу про «інтереси громадян, організацій і держави» не забути включити слово «законні» стосовно інтересів. На жаль, це саме те слово, про яке спецслужби усього світу полюбляють забувати. Хоча варто зазначити, що систематичні порушення прав людини – це скоріше результат діяльності публічної влади та публічних політиків, які прийшли до цієї влади, в руках яких спецслужби є просто інструментом.

Але, як ми вже казали, характеристика загроз інформаційній безпеці є лише одним з підходів до аналізу цієї проблеми. Це елемент «негативний», який передбачає застосування державного примусу для ліквідації загроз, їх наслідків, покарання, якщо це можливо, винних у вчиненні відповідних дій. У цьому напрямку державної діяльності цілком виправданим є принцип «меншого зла», коли задля захисту від заподіяння значної шкоди людині, суспільству, державі можливе заподіяння меншої за розміром і наслідками шкоди, введення обмежень тощо. Але розбудова концепції інформаційної безпеки лише на загро-

[1] Інформаційна безпека України. Проблеми та шляхи їх вирішення. Заочний «круглий стіл». // Національна безпека та оборона, 2001. – № 1. – С. 67.

зах, на негативі не дає можливості розвитку інформаційної сфери, не може забезпечити досягнення тих завдань, які ставляться перед державою всім ходом розвитку світових інформаційних відносин.

Досвід західноєвропейських країн, певні елементи концепції інформаційної безпеки Росії свідчать, що більш багатообіцяючим з точки зору прогресу є інший елемент інформаційної безпеки – «позитивний», який охоплює комплекс заходів щодо підвищення рівня самої безпеки. Цей елемент інформаційної безпеки охоплює значно ширший спектр суспільних відносин. Але, на нашу думку, саме тут принцип «меншого зла» застосовуватися не повинен. Адже подібні заходи не спрямовані проти конкретних загроз, а лише проти можливих. Таким чином, прямої загрози настання суспільно-небезпечних наслідків не існує. В даному аспекті повинен діяти один з головних принципів юридичної відповідальності, згідно з яким «у демократичній, соціальній, правовій державі юридична відповідальність передбачається лише за діяння, які є протиправними: за фізичні діяння (а не за думки, світогляд, особисті властивості); за суспільно шкідливі і, як правило, винні дії, що їх скоїла деліктоздатна особа»[1].

Це, зокрема, підтверджує хибність думки на зразок того, що «недостатня компетентність працівників інформаційної сфери» може кваліфікуватися як загроза інформаційній безпеці України. Адже недостатня компетентність не є підставою для настання юридичної відповідальності, інша річ, що дії посадових осіб, які відповідають за допущення недостатньо компетентних працівників до виконання функцій в сфері інформаційної безпеки, вже можуть розглядатися як такі, що становлять загрозу і знижують рівень безпеки держави.

Взагалі, на нашу думку, побудова концепції національної безпеки в сфері інформації на суто негативних засадах не відповідає тим завданням, що стоять перед нашою державою. Окрім уже зазначених недоліків, побудова системи безпеки виключно на спробах спрогнозувати загрозу автоматично ставить того, хто її застосовує, у позицію «того, хто здоганяє». Визначати на законодавчому рівні загрози, що існують або можуть постати, є абсолютно недоцільним, оскільки це має прикладний характер і ці конкретні загрози повинні виявлятися у процесі діяльності відповідних компетентних органів державної влади.

Адже існує і більш ефективний шлях. Як зазначалося в одній з розробок, «головним методом захисту важливої інформації має бути не

[1] Скакун О.Ф. Теория государства и права. – Харьков: Консум, Ун-т внутр. дел, 2000 – С. 468.

запровадження загальних переліків відомостей, які становлять державну таємницю, а конкретна інформаційна контргра щодо намірів, а не результатів їхнього втілення»[1] .

Захоплюючись аналізом конкретної ситуації, іноді забувають, що потрібно визначитися з тим, що ми, українські громадяни, суспільство та держава, хочемо досягти того, щоб відчувати себе у безпеці. І саме це бачення стану безпеки необхідно визначати за допомогою правових норм і встановлювати відповідні напрямки руху у напрямку до цієї мети.

Тож, на нашу думку, важливим є виділення напрямків інформаційної безпеки не на основі теорії загроз, адже оцінка загрози є суб'єктивним фактором, а в першу чергу виходячи з виявлення найбільш незахищених (вразливих) параметрів існування об'єктів цієї безпеки – людини, суспільства та держави, і одночасно з аналізу цілей, які стоять перед державою і суспільством.

Тож, виходячи з аналізу існуючих концепцій інформаційної безпеки та наявної нормативно-правової бази, ми пропонуємо розглядати діяльність щодо захисту інформаційної безпеки як складну систему, що включає цілий комплекс векторів державної політики. Насамперед слід виділити два комплекси питань, які диференціюються відповідно до природи правових норм, що становлять їхню нормативно-правову базу. По-перше, це комплекс питань, пов'язаних з інформаційною безпекою людини і суспільства, яка в першу чергу вимірюється ступенем свободи від втручання держави та інших осіб, можливостями самореалізації та самовизначення. По-друге, це комплекс питань, пов'язаних з інформаційною безпекою держави, які, навпаки, пов'язані із застосуванням обмежень, заборон, жорсткою регламентацією певних типів відносин в інформаційній сфері і невід'ємним елементом яких є сила державного примусу.

Комплекс питань інформаційної безпеки людини та суспільства включає такі вектори, як:

- забезпечення інформаційних прав і свобод людини і громадянина;
- захист людини від неправомірного інформаційного втручання;
- забезпечення прав націй на самовизначення в системі інформаційних відносин,
- забезпечення національної культурної і духовної ідентичності від неправомірного втручання;

[1] Національна безпека України, 1994 – 1997 рр.. Наукова доповідь НІСД. / Редкол.: О.Ф. Бєлов (голова) та ін.. – К.: НІСД, 1997. – С. 129.

• забезпечення дієздатних правових та організаційних механізмів захисту відповідних прав тощо.

Комплекс питань інформаційної безпеки держави включає такі вектори державної діяльності, як:

• безпека розвитку інформаційної сфери держави;
• захист національного інформаційного ринку;
• питання міжнародної інформаційної безпеки;
• військові аспекти інформаційної безпеки, зокрема проблеми інформаційної зброї;
• захист та обмеження обігу інформації в цілях безпеки;
• захист інформаційної інфраструктури держави тощо.

Ключову роль у проведенні політики інформаційної безпеки, особливо «силових» її векторів, повинна відігравати держава. Причому захист інформаційної безпеки повинен реалізовуватися не лише шляхом проведення політики обмеження інформаційних відносин та застосування державного примусу, а й шляхом реалізації прогностичної функції державної політики, спрямованої на підвищення рівня інформаційної безпеки. Ця політика включає в себе безпосередньо програми та плани розвитку і модернізації, що впроваджуються державою на шляху до інформаційного суспільства, а також визначення правил гри у сфері комерційних інформаційних відносин. Правові основи цієї політики включають як різного роду програми, концепції, так і конкретні нормативно-правові акти, спрямовані на проведення цієї політики в життя.

§ 3 Поняття державно-правового механізму інформаційної безпеки

Аналіз теоретичних і практичних аспектів інформаційної безпеки України дає змогу насамперед відзначити важливу роль, яку має державна діяльність в цій сфері для розбудови і зміцнення незалежної Української держави та українського народу. Забезпечення інформаційної безпеки є одним з ключових національних інтересів України. Захист інформаційної безпеки здійснюється передусім шляхом проведення зваженої і збалансованої політики держави в інформаційній сфері, яка, як ми відзначали, має три основні вектори: захист інформаційних прав та свобод людини, захист державної безпеки в інформаційній сфері та захист національного інформаційного ринку, еко-

номічних інтересів держави в інформаційній сфері, національних виробників інформаційної продукції.

Змістовий аспект політики інформаційної безпеки, як і державної політики в цілому, визначається її організаційним та регулятивно-контрольним спрямуванням. Маючи в своєму розпорядженні великий арсенал засобів, ця політика, майже за Арістотелем, є певним способом досягнення цілей держави.

Політика інформаційної безпеки держави реалізується в процесі діяльності як органів державної влади, так і недержавних інституцій. Ми можемо стверджувати, що політика інформаційної безпеки визначає зміст діяльності держави та її компетентних органів, що охоплюється відповідними аспектами інформаційної функції держави та функції національної безпеки. На сьогоднішній день значення інформаційної діяльності держави значно розширилось, навіть важко перелічити ті сфери суспільного і державного життя, на які мають вплив результати цієї діяльності: це і права людини, військова та державна безпека, економіка, культура, внутрішня та зовнішня політика тощо. Взагалі, розглядаючи проблему просторового буття держави, потрібно зазначити, що воно виходить за рамки державних кордонів. Якщо мова йде про геополітичні інтереси, про сфери впливу і т. д., то ці аспекти діяльності державного апарату виходять далеко за межі території окремої держави. Так само як абсолютно неможливо чітко обмежувати якісь сфери державної діяльності суто внутрішньою або зовнішньою спрямованістю. Тому інституціональний механізм формування політики інформаційної безпеки включає не лише внутрішньодержавні, а й міжнародні інституції.

Сама політика інформаційної безпеки складається з ряду елементів. Так, у Концепції (основах) державної політики національної безпеки 1997 року (розділ I) підкреслювалося, що «конкретні засоби і шляхи забезпечення національної безпеки України *(складовою якої є інформаційна безпека – Б.К.)* обумовлюються пріоритетністю національних інтересів, необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам загроз цим інтересам, і ґрунтуються на засадах правової демократичної держави»; а в розділі V передбачалося існування певної системи забезпечення національної безпеки, яка являє собою «організовану державою сукупність суб'єктів».[1]

[1] Постанова Верховної Ради України «Про концепцію (основи державної політики) національної безпеки України» від 16 січня 1997 р. № 3/97-ВР // Голос України – 1997. – 4 лютого. – С.5

Таким чином, ми можемо визначити три основні напрямки реалізації політики інформаційної безпеки.

По-перше, це створення нормативно-правових актів, що регулюють відповідні суспільні відносини в інформаційній сфері, встановлюють міру поведінки та відповідальність суб'єктів інформаційних правовідносин.

По-друге, це створення відповідних нових державних інституцій або введення до компетенції існуючих завдань щодо підтримання інформаційної безпеки.

І по-третє, це застосування в процесі діяльності державних інституцій конкретних, встановлених правовими нормами засобів і шляхів державного впливу на інформаційну сферу.

Визначаючи місце політики інформаційної безпеки в системі діяльності держави по виконанню своїх функцій, треба сказати, що на сучасному етапі виникає необхідність розглядати в комплексі предмет і зміст діяльності держави та засоби і способи, що її забезпечують. Це означає перехід від використання поняття функції держави до такого поняття, як державна політика, оскільки поняття функції держави розкриває лише одну із складових державної політики.

Політика являє собою організаційну та регулятивно-контрольну сфери суспільства, основні в системі інших сфер і такі, що охоплюють відносини та діяльність суб'єктів і об'єктів. Державна політика визначає зміст державної діяльності, способи її організації. Саме політика передбачає врахування та пов'язування інтересів держави з інтересами інших держав, соціальних груп та індивідів, і головне – визначення конкретного змісту та форм діяльності держави в тій чи іншій сфері.

Разом з тим сама по собі політика є надправовою категорією і регулюється правовими нормами лише у своєму зовнішньому, формалізованому вираженні. Але конкретний зміст політики, особливо державної, являє собою волю держави, спрямовану на досягнення конкретної мети. Ця воля держави закріплюється у правових нормах, здійснюється за їх допомогою у процесі діяльності державних органів та інститутів. Таким чином, з правової точки зору існує певний механізм формування і реалізації державної політики, в сфері інформаційної безпеки це державно-правовий механізм інформаційної безпеки.

Державно-правовий механізм інформаційної безпеки являє собою сукупність державних інституцій, задіяних у процесі формування і впровадження цієї політики, їх ролі та відносин, що підпорядковані чіткій ієрархії правових норм і принципів.

Цей державно-правовий механізм, відповідно до означених нами напрямків реалізації політики інформаційної безпеки, складається з трьох взаємопов'язаних елементів.

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

По-друге, це сукупність ролей та відносин, які включають правові відносини, що виникають при проведенні такої політики, та специфічні ролі, форми і методи діяльності суб'єктів проведення політики інформаційної безпеки.

По-третє, це ієрархічна сукупність правових норм та принципів, які регулюють зміст та процес проведення цієї політики, тобто ***правовий механізм інформаційної безпеки.***

Ефективність захисту інформаційної безпеки держави в цілому забезпечується ефективністю кожної складової її механізму.