

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Б. А. КОРМИЧ

ІНФОРМАЦІЙНЕ ПРАВО

Підручник

ХАРКІВ

“БУРУН і К”

2011

УДК 35.078.3 (075.8)

ББК 67.404.3 я73

К 66

*Рекомендовано Міністерством освіти і науки України як
навчальний посібник для студентів вищих навчальних закладів
(Лист №1.4/18-Г-1519 від 02.07.2008)*

*Рекомендовано до друку вченою радою Одеської національної юридич-
ної академії. Протокол №3 від 02.02.2008.*

Рецензенти:

- І. В. Арістова** – доктор юридичних наук, професор, завідувач кафедри адміністративного та інформаційного права Сумського національного аграрного університету;
- Є. В. Додін** – доктор юридичних наук, професор, Заслужений діяч науки і техніки України, завідувач кафедри морського та митного права Одеської національної юридичної академії;
- В. І. Олефір** – доктор юридичних наук, професор, завідувач кафедри адміністративного права, Вчений секретар Київського національного університету внутрішніх справ МВС України.

Кормич Б. А.

Інформаційне право.

Підручник. – Харків: БУРУН і К., 2011. – 334 с.

ISBN 978-966-8391-19-4

В підручнику аналізуються базові принципи та положення інформаційного права, його основні інститути, розглядається правове регулювання основних видів інформаційних відносин та інформаційної діяльності.

Рекомендовано студентам, аспірантам юридичних вищих навчальних закладів, а також закладів підготовки кадрів з державного управління, фахівцям та науковцям, які займаються проблемами інформаційного права, інформаційних відносин та інформаційної діяльності.

ISBN 978-966-8391-19-4

© Б. А. Кормич, 2011

© Фірма “Бурун і К”, 2011

ПЕРЕДМОВА

Одним із наслідків впливу на сучасний світ процесів глобалізації та інформатизації, бурхливого розвитку інформаційних і комунікаційних технологій є формування так званого “інформаційного суспільства”, в якому знання й інформація стають ключовими ресурсами державного і суспільного розвитку.

Ідея інформаційного суспільства, яка наприкінці 60-х – на початку 70-х років ХХ ст. була предметом обговорення науковців, нині дістала своє визнання на міжнародному і державному рівнях, про що свідчить низка міжнародних нормативно-правових актів: Декларація тисячоліття ООН; Декларація принципів ООН “Побудова інформаційного суспільства – глобальне завдання в новому тисячоріччі”; Окінавська хартія глобального інформаційного суспільства; програмні документи ОБСЄ, Ради Європи, Європейського Союзу та ін. Важливим кроком нашої держави на шляху до активного залучення в процеси розбудови інформаційного суспільства стало прийняття в січні 2007 р. Закону “Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки”.

Процеси і зміни, пов’язані з формуванням інформаційного суспільства, безумовно, кардинально підвищують суспільне значення і роль інформаційних відносин та інформаційної діяльності, що, в свою чергу, зумовлює істотне збільшення обсягів правового регулювання в цій сфері. Саме це стало однією з головних причин визнання існування галузі інформаційного права в багатьох країнах світу, зокрема і в Україні.

Відносною “молодістю” інформаційного права можна пояснити наявність багатьох прогалин і в правовому регулюванні цієї сфери та ще більше – у вивченні цієї дисципліни як галузі юридичної науки. Останніми роками в Україні й сусідній Росії створено підручники з інформаційного права та окремих його аспектів. Проте основною вадою багатьох із них є те, що деякі автори забувають, що головне призначення права – регулювання суспільних відносин, а галузевої юридичної науки – вивчення основних принципів і закономірностей такого правового впливу. Натомість, незрідка виявляється намагання “втиснути” в підручники з інформаційного права матеріал з інших галузей науки про інформацію – філософії, інформатики, кібернетики тощо, який насправді не стосується.

Саме тому виникла ідея пропонованого підручника, автори якого спробували сформулювати цілісну концепцію інформаційного права як відповідної галузі права й галузі законодавства. Поряд із викладенням теоретичних засад інформаційного права, у книзі зроблено важливий акцент на питаннях практичного застосування норм інформаційного права і державного регулювання найбільш важливих напрямів інформаційних відносин та інформацій-

ної діяльності. Концепція підручника зумовлює і його структуру. Він складається із Загальної та Особливої частин.

У розділах Загальної частини визначено основні теоретичні положення, принципи й поняття інформаційного права, специфіку основних його інститутів. Ключовим у Загальній частині є аналіз прав і свобод людини в галузі інформації та механізмів їх реалізації, які по суті є основою інформаційного права взагалі.

В Особливій частині розглянуто основні аспекти практичного регулювання інформаційних відносин та інформаційної діяльності. Відповідно до ключової класифікації інформації на відкриту та з обмеженим доступом, Особливу частину поділено на два розділи, в одному із яких висвітлено питання регулювання обігу інформації з обмеженим доступом, у другому – інформаційну діяльність у сфері відкритої інформації, зокрема, питання регулювання зв'язку й телекомунікацій, Інтернет, розповсюдження масової інформації тощо.

Для підготовки підручника використано результати досліджень у галузі правового регулювання інформаційної безпеки та інформаційного права загалом підручник “Інформаційна безпека: організаційно правові основи” та низку монографічних праць, а також досвід викладання курсів “Інформаційне право” та “Інформаційна безпека” для студентів вищих юридичних навчальних закладів.

ЗАГАЛЬНА ЧАСТИНА

РОЗДІЛ І

ПРИНЦИПОВІ ЗАСАДИ ІНФОРМАЦІЙНОГО ПРАВА

ГЛАВА 1

ОСНОВНІ ПОНЯТТЯ І КАТЕГОРІЇ ІНФОРМАЦІЙНОГО ПРАВА

*Інформація як категорія інформаційного права.
Загальні та юридичні властивості інформації.
Розвиток технологій обробки інформації та
їх вплив на інформаційні процеси. Основні
риси сучасного інформаційного суспільства.
Програмні нормативно-правові акти щодо
формування інформаційного суспільства.*

1.1. Інформація як категорія інформаційного права

Протягом усієї історії людства інформація розглядалася як важливий військовий, політичний, економічний, соціальний чинник, що значною мірою зумовлював розвиток держави, суспільства та особистості.

Володіти певною інформацією означало володіти певною цінністю суспільного характеру. Здатність індивідумів збирати, накопичувати, трансформувати й передавати інформацію стала одним із головних чинників формування людини як соціальної істоти, що дав змогу передавати досвід і знання з покоління в покоління, ставши основою суспільного прогресу. Соціальна взаємодія окремих індивідумів, соціальних груп та суспільства загалом ґрунтується передусім

на процесі обміну інформацією. Так само й соціальне управління в будь-якому масштабі пов'язане процесами збирання, оброблення та передавання інформації.

Та незважаючи на таке значення інформації для держави й суспільства, її проблеми, сутність, процеси збирання, оброблення, зберігання, передавання та розповсюдження вчені почали безпосередньо вивчати лише у ХХ ст. Інформація стала предметом окремої галузі науки – *кібернетики* (від грец. *kybernetike* – мистецтво управління), яка є наукою про загальні ознаки процесів і систем управління в технічних пристроях, живих організмах та людських організаціях.

Проте, зазначимо, що певні аспекти суспільних відносин, пов'язаних інформацією, стали предметом правового регулювання набагато раніше, ніж почали розглядатися з наукового погляду. Є, наприклад, свідчення про наявність правової регламентації такого важливого інституту інформаційного права, як державна таємниця, ще в часи Давнього Єгипту, країни Шумерів та Ассирії (IV–III тисячоліття до н. е.).

Нині є багато визначень інформації. Це можна пояснити неоднозначністю самого поняття “інформація”, а також з тим, що представники різних галузей науки та практичної діяльності по-різному сприймають це поняття інформації, що зумовлено специфічністю галузевих принципів і методів вивчення та використання інформації.

Термін “інформація” у перекладі з латинського *informatio* означає ознайомлення, викладення, роз'яснення. У загальному розумінні інформація – це певні відомості, сукупність певних даних, знань¹.

У філософській науці прийнято виділяти два аспекти існування інформації як субстанції.

По-перше, це *внутрішня* інформація, яка є мірою організації або впорядкованості системи чи процесу, їх внутрішньою характеристикою. Наприклад, цикли життєдіяльності людини, тварин і рослин регулюються певними внутрішніми механізмами.

По-друге, це *зовнішня* інформація, яка безпосередньо пов'язана з процесом *відображення* як у матеріальному, так і в нематеріальному світі. Якщо предмет зазнає певних змін, що є результатом (відображення) впливу іншого предмета, то перший предмет стає носієм інформації про другий предмет. Для неживої природи процес відображення має пасивний характер, будучи простим механізмом констатації певних даних. Для об'єктів живої природи, передусім для людини,

¹ Філософський словарь / Под ред. М. М. Розенталя. – М. : Политиздат, 1972. – С. 153

процес відображення має активний характер і пов'язаний не лише із сприйняттям інформації, але і з її аналізом та переробленням.

Засновником теорії інформації вважається К. Шеннон, який у своїй “Праці з теорії інформації та кібернетики” на початку 60-х років ХХ ст. виклав кількісно-математичні принципи інформації, вважаючи останню як “невизначеність, що скорочується”². За такого підходу кількість інформації є зворотно-пропорційною невизначеності, що усувається за допомогою цієї інформації. Теорія інформації К. Шеннона стала затребуваною із зростанням інформатизації суспільства для характеристики обсягів інформаційних потоків і згодом дала змогу розвинути нові концепції впорядкування інформаційних процесів.

Інший основоположник кібернетики – Н. Вінер розглядав інформацію як специфічну субстанцію, стверджуючи, що “інформація – це і не матерія, і не енергія”³.

Його ідеї стали основою наукової концепції, яка розглядає інформацію як основу всього існуючого, першопричину всіх явищ і процесів. Так, І. Й. Юзвішин сформулював поняття інформації як “генералізаційно єдиної первинної субстанції Всесвіту”⁴. За цим підходом усі відносини між будь-якими об'єктами та елементами (від окремих атомів та частинок до галактик і Всесвіту в цілому) ґрунтуються на процесі обміну інформацією. Отже, й сама інформація є головним ресурсом розвитку як у мікро-, так і в макросвіті, головним ресурсом розвитку людства.

Викладені вище трактування терміна “інформація” є насамперед елементами певних концептуальних підходів до універсального визначення інформації як певної субстанції та невід'ємного елемента будови світу.

Галузеві науки розглядають певні характеристики інформації, що є важливими саме для конкретної галузі знань. Так прихильники теорії інформаційної революції – американці Р. Кохане та Дж. Най поділяють інформацію, що обертається в сучасному світі на вільну інформацію, комерційну і стратегічну⁵.

² Шеннон К. Е. Работы по теории информации и кибернетике. – М., 1963.

³ Винер Н. Кибернетика и управление, их связь в животном и машине. – М.: Иностранная литература, 1958. – С. 418.

⁴ Тронь В. Феномен інформації – майбутнє Всесвіту // Вісн. Акад. держ. управ. при Президентові України. – 1998. – № 4. – С. 206.

⁵ Johnston C. B. Global news access. The impact of new communications technologies. – Westport: Praeger publishers, 1998. – p. 85.

Вільною вони вважають інформацію, що розповсюджується безкоштовно, без будь-якої матеріальної компенсації: телебачення, радіомовлення, політична реклама, різні інформаційні акції, Інтернет тощо. Стрімке, практично в геометричній прогресії, зростання потоків вільної інформації, яке має характер інформаційного вибуху, вважається одним із результатів інформаційної революції.

Комерційна інформація, тобто така, що виробляється з метою отримання прибутку у вигляді компенсації за її використання, набуває нині дедалі більшого поширення. Взагалі однією з ознак формування інформаційного суспільства є те, що інформація сама стала товаром, який має стратегічне значення для держави й суспільства.

Найбільш традиційним і звичним є третій тип інформації – *стратегічна*. Вона безпосередньо пов'язана з діяльністю держави і має такі самі давні коріння й історію, що й історія держави як правового та суспільно-політичного явища. Головною характеристикою стратегічної інформації виступає специфічний правовий режим її збирання, вироблення, зберігання та використання, а саме – режим таємності, який забезпечується силою державного примусу.

У рамках економічних відносин інформація розглядається саме з огляду на її комерційну цінність, як продукт, що має певний ціновий еквівалент або який можна обмінювати на інші товари й послуги. Як зазначають економісти, інформація є собою неречовим продуктом інтелектуальної діяльності людини і суспільства⁶. Виробництво і розповсюдження інформації нині день є одним із головних напрямів розвитку економіки.

Основним призначенням інформації є задоволення інформаційних потреб окремої людини, суспільства та держави. Саме людина є кінцевим споживачем будь-яких даних і відомостей і завдяки своєму мисленню здатна перетворити сукупність даних на те, що вважається інформацією. Досить влучним у цьому сенсі є визначення інформації, наведене в Тлумачному словнику з обчислювальної техніки, виданому у видавництві Microsoft Press: “*information* – інформація – зміст, значення даних, яке вбачають у ньому люди. Зазвичай дані складаються з фактів, які стають інформацією в певному контексті і зрозумілі людям. Комп'ютери обробляють дані без будь-якого розуміння того, чим є ці дані”⁷. Останнє речення чітко розрізняє сутність авто-

⁶ Соболев В. Информатизация и переходная инфраструктура. // Бизнес информ. – 1999. – № 3-4, с. 36.

⁷ Гостев И. М. Информационное право в России. // Конфидент. – 2000. – № 1-2. – с. 15–22.

матизованого оброблення інформації та його відмінність від розумової діяльності індивіда.

Отже, сприйняття інформації в соціальному аспекті має винятково суб'єктивний характер. Ті чи інші дані будуть становити певну інформацію для суб'єкта лише тоді, коли він здатен їх досягнути, сприйняти, інтерпретувати. Причому зміст цих даних залежатиме від особливостей і контексту сприйняття їх конкретним суб'єктом і може бути неоднаковим для різних суб'єктів. Певна інформація матиме цінність для окремого члена суспільства лише в тому разі, якщо він здатен зрозуміти її значення і використати.

Проте законодавство використовує універсальне визначення інформації, яке не залежить від її суб'єктивного сприйняття і охоплює будь-яку інформацію в державі й суспільстві, щодо якої виникають певні суспільні відносини.

Основним нормативно-правовим актом, що регулює питання інформаційних відносин в Україні, є Закон України “Про інформацію”, у якому зазначено, що *інформація – це документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі*⁸. Ключовим елементом цього визначення інформації є “*документовані або публічно оголошені відомості*”. Тобто будь-які відомості, аби стати інформацією, має набути певного зовнішнього вираження (форми) поза свідомістю людини – бути закріплені на фізичному носії (документовані) або висловлені людиною усно чи за допомогою певних технічних засобів (публічно оголошені). Сенс подання інформації у одній з таких форм полягає в тому, що тільки в такому вигляді дані стають доступними, тобто такими що можуть бути передані іншим користувачам і перетворитися на об'єкт суспільних відносин, найбільш важливі з яких стають предметом правового регулювання.

Ця характеристика ілюструється в універсальному визначенні, що його було наведено в роботі Марка Пора, присвяченій проблемам інформаційної економіки *інформацією є дані, що були організовані і передані*⁹. Процес передачі даних передбачає наявність щонайменше двох суб'єктів – того, що передає дані, й того, для кого ці дані передаються. Суб'єкт, що передає або документує дані, повинен розраховувати на те, що вони будуть кимось отримані. Так само і публічне ого-

⁸ Про інформацію: Закон України від 2 жовтня 1992 р. // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

⁹ Porat M. The Informational Economy: Definition and Measurement. – Washington D. C. : US Department of Commerce, Office of Telecommunications. – 1977. – P. 2.

лошення даних передбачає наявність суб'єктів, які їх отримують. Це означає, що як соціальна цінність інформація не може існувати поза певними інформаційними процесами – збирання, передавання, оброблення та зберігання.

Поняття інформації, визначене в Законі України “Про інформацію”, практично повністю відтворюється і в Цивільному кодексі України (ЦК). Згідно з нормою ч. 1 ст. 200 ЦК, “Інформацією є документовані або публічно оголошені відомості про події та явища, що мали або мають місце у суспільстві, державі та навколишньому середовищі”¹⁰. Єдиною різницею є застосування стосовно подій і явищ виразів *мали або мають місце* (ЦК), замість використаної в Законі України “Про інформацію” *відбуваються*, що формально розширює часові рамки. Уваги заслуговує інше. ЦК розглядає інформацію як нематеріальне благо, відмежовуючи її разом із тим від інших видів нематеріальних благ – результатів інтелектуальної і творчої діяльності та особистих нематеріальних благ. Це є важливим аспектом, оскільки інформація може бути і не бути об'єктом права інтелектуальної власності. Відповідно правові відносини в галузі інформації і правові відносини щодо об'єктів інтелектуальної власності та авторських прав мають різну природу, принципи та методи регулювання. Обґрунтуванням такої тези може слугувати норма ч. 3 ст. 200 ЦК, яка визначає, що порядок використання інформації та захисту права на неї встановлюється окремим законом, на відміну від інших видів нематеріальних благ, щодо яких є посилання безпосередньо на цивільне законодавство.

У Законі України “Про телекомунікації” дано дещо інше визначення поняття “інформація”, яке значно розширює і конкретизує перелік форм подання інформації, яка може бути об'єктом правовідносин. Згідно зі ст. 1 цього Закону, інформація – це *“відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб”*¹¹.

Отже, визначені в законодавстві форми і способи подання інформації не є вичерпними, що дає змогу визначити інформацію як *відомості, що були організовані в такій формі, документовані, передані або оголошені таким чином, що можуть бути сприйнятими іншою особою*.

¹⁰ Цивільний кодекс України № 435-IV від 16 січня 2003 р. // Відомості Верховної Ради України. – 2003. – № 40–44. – Ст. 356.

¹¹ Про телекомунікації: Закон України від 18 листопада 2003 р. № 1280-IV // Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155.

Організованість, передавання та зрозумілість даних, які існують лише в свідомості окремого індивіда або всередині якого-небудь технічного пристрою, перетворюють їх на інформацію, роблять їх придатними для суспільного використання.

Суспільне використання інформації обмежується певними правилами та законами, за якими відбуваються інформаційні процеси.

По-перше, інформаційні процеси підпорядковані законам природи (наприклад, процес розповсюдження інформації, залежно від способу, може залежати від швидкості звуку або світла, характеристик інформаційно-комунікаційних технологій або фізичних можливостей людини).

По-друге, порядок здійснення інформаційних процесів визначається соціальними нормами – нормами моралі та права.

Такими інформаційними процесами є збирання, виробництво, зберігання, використання та розповсюдження інформації.

Урегульованість інформаційних процесів соціальними нормами дає підстави говорити про таке явище, як *суспільний обіг інформації*, що охоплює інформацію, подану у формі, придатній для суспільного використання і щодо якої виникають суспільні відносини.

Одночасно в межах суспільного обігу інформації існує *правовий обіг інформації*, який охоплює лише ту інформацію, суспільні відносини щодо якої врегульовані правовими нормами. Природно, що об'єктом правового регулювання виступає не сама інформація, а певні суспільні відносини, які виникають з приводу її збирання, виробництва, зберігання, використання та розповсюдження.

Кожна конкретна інформація має також певні індивідуальні характеристики, до яких насамперед належать її кількість, зміст, цінність та якість.

Кількість інформації може виражатися як у кількісних одиницях (сторінки, байти тощо), так і в відносному вимірі (наскільки інформація знімає невизначеність).

Зміст інформації – це конкретне значення даних і відомостей у тому контексті, в якому вона є зрозумілою для особи.

Цінність інформації характеризує її суспільне значення і може виражатися як у грошових одиницях, так і у відносному значенні (важлива, неважлива тощо).

Якість інформації визначає, наскільки вона здатна задовольнити інформаційні потреби суб'єктів інформаційних відносин, і характеризується такими критеріями, як повнота, достовірність, цілісність тощо.

1.2. Загальні і юридичні властивості інформації

За визначеннями науковців, інформація є певною особливою субстанцією, яка відрізняється від матерії та енергії, тому має певні особливості та властивості, які зумовлюють специфіку інформаційних процесів. Наявність такої специфіки неодноразово підкреслювали фахівці в галузі інформаційного права, стверджуючи, що інформація будь-якого виду і призначення, яка створюється, застосовується або розповсюджується в правовій системі, має певні властивості, що тягнуть за собою певні юридичні наслідки під час обігу¹². Існує досить багато поглядів на цю проблему, оскільки інформація як об'єкт наукового дослідження та вивчення передбачає виділення семантичних, лінгвістичних, прагматичних і технічних аспектів¹³. При цьому наводяться переліки відповідних властивостей інформації. Але досить часто, в характеристики цих властивостей механічно переносяться ідеї, сформульовані в рамках природничих галузей науки і практики. Для права цікавими є саме соціальні аспекти цієї проблеми.

Узагальнюючи різні погляди на властивості інформації, вважаємо за доцільне дещо змінити акценти й класифікувати їх на дві групи – загальні та юридичні.

До *загальних властивостей інформації* належать ті, що притаманні будь-якій інформації, що використовується в суспільстві, і впливають на всі суспільні відносини щодо інформації, незалежно від наявності або відсутності правового регулювання. Такими загальними властивостями є:

Системність інформації – будь яка інформація, що створюється людиною, має певну внутрішню організаційну структуру, зумовлену виробленими в суспільстві правилами та законами. Наприклад, будь-яка фраза, речення, документ мають свої правила побудови, що визначаються граматичними та орфографічними правилами, лексикою, логікою мислення, правилами документування тощо.

Селективність інформації – залежність її від процесів її вибору та відбору є одним з ключових положень теорії інформації. Стосовно суспільних відносин щодо інформації можна стверджувати, що перетворення сукупності даних і відомостей на інформацію є суб'єктивним процесом, який залежить від суб'єкта, котрий одержує, використовує, поширює та зберігає інформацію. Тому на основі од-

¹² Копылов В. А. Информационное право. – М. : Юрист, 2002. – С. 49.

¹³ Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право. – СПб., 2001. – С. 38.

них і тих самих даних або відомостей різними суб'єктами може бути створена різна за змістом інформація, зроблені різні висновки тощо.

Субстанціональна несамостійність інформації – зумовлена зв'язком інформації з процесом відображення, за якого інформація не може існувати без її носія, що відображує той вплив, який призвів до виникнення інформації. Носієм інформації можуть бути об'єкти як неживої (предмети, випромінювання), так і живої природи (люди, тварини, рослини).

Невичерпність інформації полягає в тому, що на відміну від предметів матеріального світу, використання яких призводить до фізичного зношення або вичерпання, використання інформації не впливає на її властивості і, отже, вона може мати необмежену кількість використань та користувачів, залишатись при цьому в незмінному стані. Ця властивість інформації є однією з ключових у більшості сучасних концепцій інформаційного суспільства, оскільки дає змогу розглядати її як невичерпний ресурс і для економіки, і для діяльності публічної влади.

Здатність інформації до розповсюдження зумовлена її невичерпністю та ґрунтуванням на відображенні. У більшості концепцій інформаційного суспільства відзначається здатність інформації безконтрольно поширюватись, попри встановлені обмеження доступу до неї. Це зумовлено тим, що рух і розповсюдження інформації, передавання її від одного предмета (істоти) до іншого залежать від природних процесів відображення інформації. Тому вжиття людиною заходів щодо обмеження цього природного процесу не може бути ефективним.

Здатність інформації до трансформації полягає в тому, що інформація може зберігатися, накопичуватися на будь-яких придатних для цього носіях, а також як у свідомості окремого індивідуума, так і в масовій свідомості суспільства. Інформація здатна змінюватися, вдосконалюватися, деталізуватися; на її основі можна створювати нову інформацію і т. ін. Суб'єкт, що отримав, спожив інформацію, може передавати її іншим суб'єктам в незмінному або переробленому вигляді завдяки власному розуму або створити нову інформацію. У такому процесі передавання або поширення інформації вона, будучи отриманою іншими суб'єктами, залишається і в суб'єкта, що поширює її.

До юридичних властивостей інформації належать ті, що безпосередньо зумовлюють специфіку правового регулювання суспільних відносин щодо інформації.

Фізична невідчужуваність інформації пов'язана з ідеальною її природою і полягає в тому, що інформація не здатна відчужуватись від людини її носія. В більш широкому тлумаченні, ця властивість може бути перенесена і на юридичних осіб, суб'єктів інформаційних відносин. Це одна з головних відмінностей інформації від речей (матеріальних предметів), передавання яких від одної особи до іншої означає відчуження і втрату першою частини або всіх прав на цю річ. Під час передавання (поширення) від одної особи до іншої інформація може залишатися в обох, навіть виробник інформації здебільшого зберігає комплекс авторських прав на інформацію. Отже, передавання інформації від однієї особи до іншої, з правового погляду замінюється і оформляється передаванням чітко визначеного комплексу прав на цю інформацію.

Необхідність відособлення інформації – ґрунтується на законодавчому її розумінні як документованих або публічно оголошених відомостей, яке передбачає, що для залучення у врегульований правом обіг інформація має бути відокремлена від її виробника способом подання її у формі сигналів, знаків, звуків, рухомих або нерухомих зображень чи іншим способом і в такій формі передана іншим суб'єктам інформаційних відносин.

Незалежність прав на інформацію та на її матеріальний носій – юридична властивість інформації, що захищена правом інтелектуальної власності і полягає в тому, що інформація на матеріальних носіях одночасно є інформацією (змістом) та матеріальним носієм. У більш загальному розумінні можна сказати, що право на інформацію і право власності на матеріальний носій інформації не залежать одне від одного. Відчуження матеріального носія не означає відчуження права на інформацію і навпаки. Понад те інформація є нематеріальним благом, а матеріальний носій – річчю, тому йдеться про різні типи правового регулювання. Такий саме підхід можна застосовувати щодо аналізу правового регулювання трансляції інформації за допомогою телебачення або радіомовлення. Адже при цьому також окремо регулюються питання правових відносин щодо інформації як продукту та інформаційної діяльності як доведення інформації до споживача.

Здатність до тиражування – це властивість інформації, котра безпосередньо пов'язана з такою її характеристикою, як невичерпність. Ця властивість є ключовою для правового регулювання діяльності щодо розповсюдження інформації, адже останню можна копі-

ювати (тиражувати) необмежену кількість разів, і при цьому вона не зменшується в обсязі і не втрачає своїх споживчих якостей. Важливим є те, що видатки на створення інформації (першого примірника) можуть бути набагато більшими, ніж видатки на створення кожного наступного примірника (тиражу). Фактично на цій особливості інформації ґрунтуються галузі економіки, пов'язані із виробництвом та розповсюдженням інформації. В цьому також полягає економічна привабливість порушень авторських прав, адже відпадає потреба витрачатись на створення первинної інформації. Тому такою актуальною нині є проблема встановлення й захисту майнових прав на інформацію.

1.3. Розвиток технологій оброблення інформації і їх вплив на інформаційні процеси

Із розвитком інформаційних та комунікаційних технологій пов'язана більшість змін на шляху до інформаційного суспільства. Вважається, що так само, як у XVII ст., промислова революція змінила тогочасний світ і стала економічною базою для народження нового економічного укладу – капіталізму (чи індустріального суспільства), нині відбувається так звана “інформаційна революція”, яка змінює традиційні схеми загальної взаємозалежності постійним збільшенням кількості каналів комунікації у світовій політиці та економіці і стає передумовою становлення й розвитку нової формації – інформаційного (постіндустріального) суспільства.

Поширеною є також думка, що тепер світ переживає п'яту технологічну революцію в галузі обміну інформацією¹⁴. Причому, кожна з п'яти технологічних революцій значною мірою змінила не лише засоби здійснення комунікації та інформаційних процесів у суспільстві, а й саму сутність цих процесів та їх сприйняття людиною. Це технологічні революції:

1456 р. – винахід друкарського верстата (Йоганн Гуттенберг). Із суто технічного погляду було створено засіб багаторазового тиражування інформації на паперових носіях, які були ідентичними. Але цілий ряд дослідників відмічає що розвиток видавничої справи докорінно змінив цілу низку сфер людського життя. Так, було створені передумови для поширення письменності, розвитку освіти, науки, літератури, друкованих засобів масової інформації тощо. Більше того, видавнича справа сформувала цілий стиль мовлення та мислення, послі-

¹⁴ Бачило І. Л., Лопатин В. Н., Федотов М. А. Информационное право. – СПб., 2001 – С. 52–53.

довного та зв'язаного законами логіки, який сьогодні називають літературною та науковою мовою.

1876 р. – створення телефонного апарата (Олександр Белл, США). Разом із телеграфом телефон докорінно змінив комунікаційні процеси, дав змогу передавати інформацію на відстані зі швидкістю світла. Завдяки цьому стала можливою комунікація на відстані у режимі реального часу. Це істотно змінило організацію всіх видів соціального управління, у багато разів пришвидшило всі інформаційні процеси. Адже до цього швидкість передавання інформації здебільшого була обмежена швидкістю пересування транспортних засобів.

1895 р. – створення радіо (А. Попов, Г. Герц, Г. Марконі, Н. Тесла). Радіотрансляція дає змогу передавати інформацію за допомогою хвиль, які вільно поширюються в навколишньому середовищі, і перше, створює умови для зв'язку з будь-якою точкою планети і за її межами. Радіо зробило можливим передавання інформації необмеженій кількості користувачів, що стало новим етапом у розвитку такого її виду, як масова інформація.

1930 р. – створення телебачення, винахід кінескопа (В. Зворикін, США). Телебачення не тільки стало принципово новим засобом інформації, а й сприяло формуванню істотно нового типу сприйняття інформації. В зарубіжній соціології поширена думка, що телебачення сприяло переходу від “інформаційної галактики Гуттенберга, до галактики Маклюєна” (М. Маклюєн – канадський учений, що одним із перших звернув увагу на соціальний ефект нових засобів інформації і телекомунікації). Як уже зазначалося, видавнича справа зумовила логічний тип сприйняття друкованої інформації. Телебачення ж впливає на глядача аудіовізуальними образами – сукупністю рухомих зображень та звукової інформації, що, на думку вчених, призводить до емоційного типу сприйняття інформації.

1945 р. – створення ЕОМ (Дж. Моклі, Д. Еккерт, Пенсільванський університет, США). Електронно-обчислюванні машини відкрили новий етап розвитку інформаційних технологій у зв'язку із поширенням автоматизованої обробки інформації. Саме цей чинник значно підвищив ефективність інформаційної діяльності, пришвидшив темпи збільшення кількості інформації, що виробляється суспільством. Поява на початку 80-х років XX ст. певною мірою доступних персональних ЕОМ відкрила шлях до процесу масової інформатизації, а розвиток телекомунікаційних мереж, який розпочався наприкінці 70-х років, сприяв появі Інтернет, що став одним із ключових елементів інформатизації та комунікації нового типу.

Проте, зрозуміло, що сама по собі інформаційна технологія не може змінити життя людини, суспільства й держави у кращий чи гірший бік. Результати запровадження будь-якої технології залежать від багатьох суб'єктивних та об'єктивних чинників і насамперед від мети і способів її застосування людьми. Таке твердження яскраво ілюструється запропонованим не так давно М. Кранцбергером законом відносин між технологією і суспільством: “Перший Закон Кранцберга наголошує, що технологія є ні гарною, ні поганою, ні нейтральною”¹⁵. Тобто будь-яка технологія початково не чинить ні негативного, ні позитивного впливу. Наслідки від її застосування залежать передусім від його мети, яка, у свою чергу залежить від людської природи. В цьому аспекті, наприклад, середньовічні шпигуни нічим не відрізнялися від сучасних, або загальна мета пропаганди 30-40 років ХХ ст. не відрізнялися від сучасної. Застосовуються лише нові способи і методи вирішення старих завдань. І це призводить до того, що технологія, змінюючи та розширюючи можливості, деякою мірою змінює і свідомість людини.

Складний механізм впливу інформаційних технологій на суспільство підкреслює і відомий теоретик інформаційного суспільства М. Кастельс. Зокрема, він говорить про “всеосяжність ефектів нових технологій. Оскільки інформація є інтегральною частиною будь-якої людської діяльності, всі процеси нашого індивідуального і колективного існування безпосередньо формуються (хоча, безумовно, не детермінуються) новим технологічним способом”¹⁶.

1.4. Основні ознаки сучасного інформаційного суспільства

Наприкінці ХХ ст. сталися значні зміни у сприйнятті самого поняття інформації та її соціального значення в суспільстві. Це пов'язано з процесом формування так званого інформаційного суспільства, тобто суспільства, основною характеристикою якого є стрімке зростання всепроникної інформації про всі сторони його життєдіяльності. Нині термін “інформаційне суспільство” є визнаним як у

¹⁵ *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

¹⁶ *Кастельс М.* Информационная эпоха: экономика, общество, культура: Пер. с англ. / Науч. ред. О. И. Шкарагана – М. : ГУ ВШЭ, 2000. – С. 77.

рамках різних галузей науки, так і на державному рівні і закріпленій у низці міжнародних та національних нормативно-правових актів. Проте розглядати інформаційне суспільство слід не як явище, що вже відбулося, а як процес, що пов'язаний із різними сферами життєдіяльності людства – економікою, правом, організацією публічної влади, політикою, соціальною сферою та ін. З одного боку, процес формування інформаційного суспільства є одним із елементів більш обсягового явища – глобалізації, з другого – цей процес в різних державах відбувається різними темпами. Насамперед він охоплює економічно розвинені країни, які за показниками інформатизації суспільства перебувають в авангарді світової цивілізації. І хоча досі ще немає єдиного, універсального визначення інформаційного суспільства, можна виокремити кілька аспектів його формування й ті зміни, що відбуваються в різних сферах життєдіяльності держави та суспільства.

У первинному значенні термін “інформаційне суспільство” було застосовано в економічному аспекті для пояснення якісних змін у структурі валового внутрішнього продукту (ВВП) економічно розвинених країн, які почали виявлятися ще в 60-і роки XX ст. Ці зміни полягали у зростанні відсотка ВВП, у нематеріальній сфері виробництва, зокрема стосовно інформаційного продукту і послуг. Вперше термін “інформаційне суспільство” вжив американський економіст Ф. Машлуп у праці “Виробництво і поширення знання у Сполучених Штатах” (1962), хоча сам процес трансформації структури виробництва в розвинених державах почали виявляти японські та американські економісти наприкінці 50-х років XX ст. В економічному контексті синонімом терміна “інформаційне суспільство” є терміни “посткапіталістичне”, “постіндустріальне” суспільство, в яких в економіці починає переважати виробництво не матеріальних товарів а інформації і знань (Д. Дарендорф, 1958). Причому в такому суспільстві інформація починає контролювати не тільки бізнес, а й державу (Дж. Гелбрейт, 1967). Нині процес формування інформаційного суспільства став об'єктивним для економічно розвинених країн (насамперед США, Японії, Канади, країн Європейського Союзу), економіку яких формують сфера послуг, високі технології і виробництво інформаційної продукції. Крім того матеріальне виробництво переноситься у країни, що розвиваються, з більш дешевою і менш кваліфікованою робочою силою. При цьому постійно спостерігається збільшення економічного, технологічного та інформаційного розриву між країнами-лідерами та іншими, який стає практично нездо-

ланним. Це явище дістало назву “технологічного розвитку, що вилучає”, тобто розвитку, що призводить до вилучення певних суспільних верств, суспільств, територій і держав з нової глобальної системи інформаційних зв’язків та економічних відносин, залишаючи їх на “узбіччі цивілізації”¹⁷.

Істотні зміни в економічному житті, безумовно впливають і на суспільство та державу. Головними аспектами соціального та політичного обличчя і рівня розвитку такого суспільства є: “інформованість населення, безперешкодна робота всіх служб масової інформації та їх здатність збирати і передавати об’єктивні відомості і їх оцінки, а також інтерес їх до роботи у всіх верствах народу, доступність інформації та наявність технічних засобів, що дають змогу отримати її”¹⁸. Тобто в інформаційному суспільстві інформація є ресурсом не тільки економічного, а й соціального, політичного та культурного розвитку. Окремі члени суспільства не тільки мають можливість вільно отримувати інформацію й користуватися засобами інформації та комунікації, а й зацікавлені в отриманні та розповсюдженні інформації, широко її використовують і беруть активну участь в інформаційних процесах. Це, в свою чергу, сприяє значному збільшенню кількості інформації, яку виробляє людство. Крім того, має значення здатність інформації до швидкого розповсюдження. Нині незаперечним є факт, що одночасно зі зростанням темпів розвитку суспільства і технологій зменшується час, протягом якого держава здатна забезпечувати секретність тієї чи іншої інформації, і це не в останню чергу пов’язано зі специфікою такої субстанції, як інформація. На думку Х. Клівленда, “подібно до вірусу інформація намагається уразити все навколо себе. Найсуворіші бар’єри таємності, права інтелектуальної власності, а також питання конфіденційності будь якого рівня легко долаються за допомогою цього всесильного ресурсу”¹⁹.

Із зазначеним вище тісно пов’язаний і політико-правовий аспект формування інформаційного суспільства. За визначенням І. В. Арістової, інформаційне суспільство є громадянським суспільством з розвитком інформаційним виробництвом і високим рівнем інформаційно-правової культури, в якому ефективність діяльності людей забезпе-

¹⁷ Див.: Кастельс М. Информационная эпоха: экономика, общество, культура: Пер. с англ. / Под. науч. ред. О. И. Шкаратана. – М. : ГУ ВШЭ, 2000 – С. 23.

¹⁸ Политология: Энциклопедический словарь / Общ. ред. и сост. Ю. И. Аверьянов. – М., 1993. – С. 130.

¹⁹ Cleveland H. The knowledge executive. Leadership in an information society. – New York: Truman Talley books, 1989. – P. 32.

чується розмаїттям послуг на основі інтелектуальних інформаційних технологій і технологій зв'язку²⁰. Інформаційне суспільство може розвиватися лише в умовах правової демократичної держави та розвинутого громадянського суспільства, адже ключовим у його формуванні є можливість вільного отримання та розповсюдження інформації, що може бути забезпечена лише за неухильного додержання прав і свобод людини, демократичної форми правління, дієвого контролю та участі інститутів громадянського суспільства. Деякі дослідники інформаційного суспільства зазначають, що фатальне економічне відставання колишнього СРСР та інших соціалістичних країн багато в чому було зумовлене закритим типом суспільства, в якому не існувало вільного обігу інформації. Відповідно в цих країнах не могли вільно розвиватися інформаційні відносини, що зробило неможливим процес інформатизації та перехід від економіки індустріального типу до інформаційної (постіндустріальної).

Процес формування інформаційного суспільства не оминув свої впливом і такий інститут, як держава та її публічна влада. Цей вплив характеризується терміном “зсув влади”, під яким розуміють зміну акцентів у засобах управління в бік широкого використання інформації. Відомий американський учений А. Тоффлер в одній зі своїх праць висловлює сучасні погляди на значення інформації для функціонування системи публічної влади. Зокрема, він підкреслює, що тепер традиційна система влади, що ґрунтується на силі та багатстві, вже втрачає свою ефективність. На його думку, суб'єкти управління “виявили, що більше ніхто не бажає сліпо підкорятися, як це було раніше. Підлеглі задають питання і вимагають відповіді на них. Відбулася революція в самій природі влади. Зсув влади – це не просто її зміна, це її перетворення”²¹.

А. Тоффлер виділяє три компоненти влади: силу, багатство і знання, що в принципі є трансформацією більш звичної класифікації методів управлінського впливу на примус, заохочення та переконання, тільки в цьому разі йдеться не про самі методи здійснення влади, а про владні ресурси, що лежать в основі відповідних методів. Він, зокрема, зазначає, що знання, сила та багатство, відносини між ними визначають владу в суспільстві. Френсіс Бекон сказав “знання – сила”,

²⁰ Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти. – Х.: УВС, 2000.

²¹ Toffler A. Powershift. Knowledge, wealth, and the violence at the edge of the 21 century. New York: Bantam books, 1990. – Р. 4.

але він не згадав про її якість, про значення його зв'язку з іншими значущими ресурсами влади²².

Для аналізу можливостей використання відповідних владних ресурсів важливими чинниками є рівень їх доступності та наявності в управлінському арсеналі. Як влада, так і багатство є обмеженими та вичерпними ресурсами, що призводить до наявності відповідних обмежень їх використання. Як застосування сили має певні обмеження та вичерпує значні ресурси (людські, технічні, матеріальні), так і застосування багатства обмежене розмірами наявних фінансових ресурсів. Інформація ж, навпаки, є невичерпним ресурсом через її властивість копіювати саму себе будь-яку кількість разів. При застосуванні такого владного ресурсу, як знання чи інформація, витрачається не сам ресурс, а лише наявні витрати на функціонування засобів комунікації і тиражування носіїв інформації.

Однією з основних ознак сучасної державної влади є її інформаційно-інтелектуальний характер, що виявляється у певних її характеристиках:

- будь-які процеси організації вимагають інформаційного забезпечення, наявність повних достовірних відомостей про об'єкт і середовище, в якому той перебуває;
- інформація забезпечує життєздатність влади, її стійкість;
- “хто володіє інформацією, той володіє владою”;
- інформація виступає як ефективний засіб формування інтелектуального потенціалу держави;
- інтелект (розум, знання) є головною основою процесу реалізації влади, без знань неможливо раціоналізувати й цілеспрямовано здійснювати політику²³.

Одним із ключових аспектів формування інформаційного суспільства є *технологічний*, який полягає у створенні й запровадженні нових інформаційних та інформаційно-телекомунікаційних технологій. У 1993 р., офіційно проголошуючи завдання розбудови інформаційного суспільства в Європі, Комісія ЄС, зокрема, визначила, що інформаційне суспільство – це суспільство, в якому діяльність людей відбувається на основі використання послуг, що надаються за допомогою інформаційних технологій і технологій зв'язку²⁴.

Ще одним аспектом формування інформаційного суспільства за

²² Там само. – Р. 16.

²³ Политология / Отв. ред. В. Д. Перевалов. – М. : Изд. группа НОРМА-ИНФРА, 1999. – С. 75.

²⁴ Європа на шляху до інформаційного суспільства // Матеріали Європейської Комісії 1994 – 1995 рр. – К.: Держкомзв'язку та інформатизації України, 2000. – С. 3.

умов застосування новітніх інформаційних технологій є його *глобальний характер*. Сучасні інформаційні технології вже не обмежуються рамками однієї країни, а мають загальносвітове значення. Це зумовлює збільшення темпів життя держави і суспільства та “стискає” наш світ, роблячи його маленьким з огляду на інформаційні відносини та інформованість людини. На думку канадського вченого Маршала Маклюєна, інформаційна ситуація світу схожа на велике селище. Події, що відбулися в найвіддаленішому регіоні планети, в той самий день стають відомими людям у всіх цивілізованих країнах. Електронні засоби масової комунікації та передачі інформації діють зі швидкістю світла, тим самим стираючи кордони та зменшуючи відстані. Завдяки розвитку сучасних інформаційних технологій інформація з будь-якого кутка нашої планети може за лічені секунди бути передана в будь-яку іншу точку земної кулі. Таким чином в інформаційному суспільстві суттєво змінюються уявлення про час і відстань, які у сприйнятті людини “стискаються”.

Розвиваючи цю ідею, М. Кастельс підкреслює, що всі культури створені із комунікативних процесів, а відповідно, всі форми комунікації ґрунтуються на виробництві і споживанні знаків, тобто всі реальності передаються через систему символів. Отже, людина сприймає не саму реальність, а певну, прийнятну для її культури систему символів які передають цю реальність. Отже, “в людській, інтерактивній комунікації, незалежно від засобів, усі символи дещо зміщені відносно їх символічного значення. В певному сенсі *вся реальність сприймається віртуально*²⁵. Причому така ситуація повністю відбиває етимологічне значення цих термінів: віртуальний (*virtual*) – такий, що існує на практиці, хоча не строго в заданій формі або не під певним ім'ям, а реальний (*real*) – фактично існує²⁶.

Отже, М. Кастельс вважає, що нова комунікаційна система, на відміну від історичного досвіду, створює *реальну віртуальність*, яка визначається як система, в якій сама реальність (тобто матеріальне/символічне існування людей) повністю схвалене, повністю занурене в віртуальні образи, у вигаданий світ, світ, у якому зовнішні зображення перебувають не просто на екрані, через який передається досвід, але

²⁵ Кастельс М. Информационная эпоха: экономика, общество, культура: Пер. с англ. / Под науч. ред. О. И. Шкаратана. – М.: ГУ ВШЭ, 2000. – С. 351.

²⁶ Див.: Oxford Dictionary of Current English. – Oxford: Pergamon Press, 1992.

й самі стають досвідом²⁷. Фактично можна говорити, що сучасна людина живе у світі, більшу частину якого вона не здатна обстежити за допомогою власного досвіду, тому уявлення і окремої людини і соціальних груп формуються завдяки передаванню чужого досвіду через комунікативні канали – друковані видання, телевізійні чи радіопрограми, документи, мульти-медіа тощо.

Подібна нова система комунікації здатна руйнувати звичну послідовність подій, адже минуле, сьогодення і майбутнє можуть бути об'єднані і взаємодіяти в одному повідомленні, що дає змогу говорити про “позачасовий час, який належить до простору потоків”²⁸ і який залежить виключно від того, ким програмується послідовність передач інформації або повідомлень.

Подібні, ще до кінця не осмислені, зміни, в комунікаційних та інформаційних процесах, а особливо їх темпи і обсяги, дають підстави стверджувати, що традиційні підходи до проблеми забезпечення інформаційної безпеки з кожним днем втрачають свою ефективність.

Проте зміни, що відбуваються завдяки формуванню інформаційного суспільства, можуть мати як позитивні, так і негативні наслідки. Адже реформування держави, економіки й суспільства в напрямі орієнтації на використання інформаційного ресурсу як основного ресурсу та засобу регулювання само по собі не гарантує ані демократії, ані процвітання. Навпаки, за деякими концепціями, розвиток у геометричній прогресії засобів масової комунікації призвів до виникнення такого суспільного феномена, як *інфократія*, що означає владу інформації²⁹. Завдяки розвитку засобів комунікації та інформаційних технологій влада дістала можливість, по-перше, здійснювати тотальний контроль за збиранням інформації щодо своїх громадян, по-друге, маніпулювати свідомістю мас. Це може призвести до обмеження громадянських прав і свобод людини і навіть до нового типу диктатури чи принаймні до порушень рівноваги між дефініціями “інститути держави” і “інститути громадянського суспільства”.

Можливості влади контролювати власних громадян справді збільшилися і не стільки внаслідок застосування спеціальних технологій збирання інформації, скільки внаслідок змін, яких зазнає суспільство в процесі інформатизації. Введення систем електронних розрахунків,

²⁷ Кастельс М. Информационная эпоха: экономика, общество, культура: Пер. с англ. / Науч. ред. О. И. Шкаратана. – М.: ГУ ВШЭ, 2000. – С. 351–352.

²⁸ Там само. – С. 433.

²⁹ Политология: Энциклопедический словарь / Общ. ред. и сост. Ю. И. Аверьянов. – М., 1993. – с. 129.

розвиток електронних засобів комунікації значно спрощують процедури контролю за діяльністю громадян та їх переміщенням.

Пріоритет у застосуванні органами публічної влади інформаційного ресурсу як засобу переконання також не завжди відображає демократичну сутність цієї влади. Засоби масової комунікації (преса, радіо, телебачення) – один із масових процесів виробництва інформації, розрахований на передачу інформації не для окремих осіб, а для “маси” – специфічного стихійного угруповання індивідів. Незрідка саме засоби масової комунікації і стають інструментом формування і відтворення такої маси й передачі їй певних моделей поведінки. Засоби масової комунікації стали вагомим інструментом концентрації політичної влади завдяки своїй здатності охопити більшу частину суспільства та пристосувати будь-які ідеї до середнього загального рівня сприйняття. Недаремно пресу називають “четвертою владою”, але такі функції вона може виконувати лише в умовах її реальної незалежності або альтернативності джерел інформації та їх конкуренції в суспільстві. Тоді засоби масової комунікації справді стають одним із атрибутів громадянського суспільства. За монополізації засобів масової комунікації виникає така сама ситуація, як і в разі монополізації чи узурпації державної влади. Масова комунікація перетворюється на інструмент маніпулювання свідомістю мас, стає основою концентрації та зростання державної влади.

Ще один аспект небезпеки полягає якраз в описаній вище вищезгаданій моделі “реальної віртуальності”, котра істотно змінює сприйняття людиною навколишнього світу. Одним із перших на цю особливість звернув увагу американській дослідник Г. Шиллер ще в 1980 р. У своїй праці “Маніпулятори свідомістю”³⁰ він обґрунтовував наявність глобальної маніпуляції за допомогою інформаційних потоків, що здійснюється урядами та великими корпораціями, інструментом якої виступають ЗМІ. Зміст цієї маніпуляції полягає у глобальній морфологізації всіх аспектів життя людства. Створюються певні образи, які сприймаються людиною і цілими соціальними групами, причому дуже часто на рівні підсвідомого; особисті оцінки і думки замінюються нав’язаними, і все це примушує людину вчиняти конкретні дії. За Г. Шиллером, подібний механізм є єдиним як для комерційної, так і для політичної реклами або пропаганди. Зокрема, зазначав, що насправді реклама переважно не демонструє споживчі якості товару, а нав’язує певне уявлення про стиль життя, що є атрибутом володін-

³⁰ Шиллер Г. Маніпуляторы сознанием. – М. : Мысль, 1980.

ня тим чи іншим товаром, потреби в цьому товарі для підтвердження певного соціального статусу. Отже, система реклами загалом, а також індустрія розваг фактично маніпулюють свідомістю окремої людини і масовою свідомістю, створюючи і нав'язуючи вигадану картину стилю життя, підсвідомо примушуючи наслідувати її. А це може мати досить негативні наслідки для суспільної моралі і традиційної побудови суспільства.

У практиці формування інформаційного суспільства в різних країнах виділяють три основні моделі: європейську, американську та азіатську³¹, які розрізняються спрямованістю здійснюваних перетворень, формами та способами участі в них держави, особливостями взаємодії між основними суб'єктами інформаційних відносин.

Європейська модель розвитку інформаційного суспільства характеризується насамперед соціальною орієнтованістю та активним залученням держави та міжнародних інституцій. Так, органи ЄС реалізують низку програм розбудови інформаційного суспільства та створення Єдиного європейського інформаційного простору. Ці програми орієнтовані на забезпечення прав і свобод громадян, розвитку інформаційної інфраструктури, вільного доступу до неї та інформованості суспільства, створення пільгових умов для розвитку підприємництва у сфері інформаційних технологій.

Американська модель розвитку інформаційного суспільства ґрунтується на популярній у США концепції “мінімальної держави”. За цієї моделі основне навантаження щодо інформатизації, розвитку інформаційної інфраструктури та й загалом щодо формування ідеології і програм інформаційного розвитку припадає на приватний сектор. Держава насамперед забезпечує регулювання інформаційної діяльності, вільну конкуренцію, бере участь у реалізації найбільш масштабних проєктів, здійснює інформатизацію публічної влади тощо. З огляду на передову роль приватного сектора, ця модель є більш комерціалізованою, орієнтованою не на вирішення соціальних і суспільних завдань, а на насичення ринку комерційними інформаційними продуктами та послугами, розвиток шоу-бізнесу тощо.

Азіатська модель інформаційного суспільства зумовлена, насамперед специфікою відповідної філософії і традицій побудови державної влади, бізнесу, суспільних відносин. Відповідно більшість завдань з інформатизації вирішується у межах взаємодії держави і великих

³¹ Див.: Бачило І. Л., Лопатин В. Н., Федотов М. А. Информационное право. – СПб., 2001 – С. 52–53.

корпорацій. Приділяється також увага забезпеченню повсякденних потреб суспільства, доступності інформаційних продуктів і послуг.

1.5. Програмні нормативно-правові акти щодо формування інформаційного суспільства

Важливою особливістю сучасних процесів глобалізації та інформатизації є так званий “економічний і технологічний розвиток, що включає”, сутність якого полягає у постійному збільшенні розриву між розвиненими країнами та рештою країн світу, внаслідок чого перші користуються перевагами зазначених вище процесів, а другі ще більше відчувають їх негативні наслідки. І така диверсифікація спостерігається не тільки між різними державами, а й усередині суспільства кожної держави. Одні соціальні групи активно залучаються до трансформаційних процесів, інші, навпаки, залишаються осторонь їх.

Тому нині загальновизнаною є потреба в активному втручанні та контролі з боку окремих держав і міжнародної спільноти, аби явища глобалізації та інформатизації позитивно впливали на кожну державу і світ у цілому. Одним із способів такого впливу стало прийняття низки програмних документів, що визначають цілі і завдання держав у формуванні глобального інформаційного суспільства. Подібні акти на міжнародному рівні було прийнято в рамках ООН, ОБСЄ, Ради Європи. Крім того, нині більшість держав, зокрема й Україну, створили національні нормативно-правові акти з питань розбудови інформаційного суспільства.

Одним із перших міжнародно-правових актів, яким зроблено спробу накреслити основні принципи і шляхи формування та розвитку інформаційного суспільства, безперечно є “Хартія глобального інформаційного суспільства”, прийнята лідерами “сімки” найбільш розвинених держав світу в Окінаві 22 липня 2000 р.³² Згідно з положеннями цієї Хартії (п. 2), сутність стимульованої інформаційно-комунікаційними технологіями (ІТ) економічної й соціальної трансформації полягає в її здатності сприяти людям і суспільству у використанні знань та ідей. Інформаційне суспільство, як його розуміють автори Хартії, дає змогу людям використовувати свій потенціал і реалізовувати свої устремління.

³² Хартія Глобального інформаційного общества. Принята 22 июля 2000 г., Окинава. // Информатизация. Дипломатия. Психология. – М.: Известия, 2002. – С. 602–610.

У Хартії також визначено, що головним принципом формування є те, що “всі люди скрізь, без винятку, повинні мати можливість користуватися перевагами глобального інформаційного суспільства”, а стійкість цього суспільства – ґрунтується на демократичних цінностях, таких як вільний обмін інформацією і знаннями, взаємна терпимість і повага до особливостей інших людей.

При цьому сама Хартія (п. 5) розглядається передусім як заклик до всіх як у державному, так і в приватному секторах ліквідувати міжнародний розрив у галузі інформації і знань. Для виконання цього завдання пропонується (п. 6) будувати роботу у таких ключових напрямках:

- проведення економічних і структурних реформ з метою створення обстановки відкритості, ефективності, конкуренції і використання нововведень;
- раціональне управління макроекономікою, що сприяє більш точному плануванню з боку ділових кіл і споживачів, і використання переваг нових інформаційних технологій;
- розроблення інформаційних мереж, що забезпечують швидкий, надійний, безпечний та економічний доступ за допомогою конкурентних ринкових умов;
- розвиток людських ресурсів, що відповідають вимогам, за допомогою освіти і постійного навчання та задоволення зростаючого попиту на спеціалістів ІТ у багатьох секторах економіки;
- активне використання ІТ в державному секторі, сприяння наданню в режимі реального часу послуг, потрібних для підвищення рівня доступності влади для всіх громадян.

У процесі розбудови інформаційного суспільства одним з головних завдань держави на національному рівні визначається (п. 19-а) вдосконалення системи управління, формування нових методів комплексного розроблення політики й відповідного нормативного забезпечення.

Певні цілі й завдання формування інформаційного суспільства сформульовано в Декларації тисячоліття ООН³³, яка, безсумнівно, є програмним документом, що визначає основні цілі та принципи міжнародного співробітництва у ХХІ ст.

У ній, зокрема, зазначається (п. 5), що головним завданням міжнародної спільноти, є забезпечення умов, за яких стала б позитивним

³³ Декларація тисячоліття Організації Об’єднаних Націй. Затверджена резолюцією 55/2 Генеральної Асамблеї ООН від 8 вересня 2000 р. // A/RES/55/2.

фактором для всіх народів у світі. Це пов'язано з тим, що, хоча глобалізація відкриває широкі можливості, її благами користуються досить нерівномірно й нерівномірно розподіляють витрати на неї. Задля вирішення цього завдання в Декларації визначений головні цілі, яким держави-учасниці надають особливого значення. Серед таких цілей деякі стосуються безпосередньо розвитку інформаційної сфери. Зокрема, визначено, що міжнародна спільнота повинна:

- вжити заходів щодо того, щоб усі могли користуватися благами нових технологій, особливо інформаційних і комунікаційних, відповідно до рекомендацій, що містяться в Декларації міністрів на сесії Економічної і соціальної ради ООН (ЄКОСОС) 2000 р. (п. 20);
- забезпечити свободу ЗМІ у виконанні ними своєї функції, а також право громадськості на доступ до інформації (п. 25).

На розвиток положень Декларації тисячоліття, держави-члени ООН під час проведення в Женеві 10–12 грудня 2003 р. першого етапу Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства було прийнято міжнародно-правовий акт під назвою “Декларація принципів побудови інформаційного суспільства – глобальне завдання в новому тисячолітті”³⁴. Основною метою цієї декларації, як зазначено в її п. 2, є використання потенціалу інформаційних і комунікаційних технологій для досягнення сформульованих у Декларації тисячоріччя цілей розвитку.

У контексті цієї мети учасники Декларації заявили про своє загальне прагнення й рішучість побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток інформаційне суспільство (п. 1).

За своєю структурою Декларація складається з трьох основних розділів, у яких визначаються певні узгоджені позиції, спільні цілі та спільні обов'язки держав-учасниць.

У розділі А “Наша загальна концепція інформаційного суспільства” викладено переваги та небезпеки, пов'язані з формуванням інформаційного суспільства, декларується необхідність здійснення всіх пов'язаних з цим процесів у повній відповідності з принципами та цілями ООН, захистом прав і свобод людини, розбудовою інформаційного суспільства на благо нинішнього та майбутнього поколінь.

Зокрема, визначено, що фундаментом інформаційного суспільства

³⁴ Декларація принципів “Побудова інформаційного суспільства - глобальне завдання в новому тисячолітті”. – Женева. 12 грудня 2003 р.

є проголошене в ст. 19 Загальної декларації прав людини право кожної особи на волю переконань і на вільне їх вираження. Кожний, де б він не перебував, повинен мати можливість брати участь в інформаційному суспільстві, і нікого не можна позбавити пропонуваним цим суспільством переваг (п. 4).

Важливим є застереження, що інформаційно-комунікаційні технології (ІКТ) слід розглядати як інструмент, а не як самоціль (п. 9). Тобто основною метою розбудови інформаційного суспільства є задоволення потреб окремих індивідів, суспільства та держави. А ІКТ виступають лише потужним інструментом підвищення продуктивності, економічного зростання, створення нових робочих місць і розширення можливостей працевлаштування, а також підвищення якості життя для всіх.

У розділі В Декларації “Інформаційне суспільство для всіх: основні принципи” визначено ключові принципи побудови відкритого для всіх інформаційного суспільства:

1) *сприяння органів державного управління й усіх зацікавлених сторін застосуванню ІКТ із метою розвитку*. Підкреслено, що органи державного управління, приватний сектор, громадянське суспільство, міжнародні організації мають відігравати важливу роль у розвитку інформаційного суспільства, брати на себе відповідальність за це і за можливість брати участь у процесах ухвалення рішень;

2) *інформаційна та комунікаційна інфраструктура – необхідний фундамент відкритого для всіх інформаційного суспільства*. Це забезпечується проведенням політики, що створює на всіх рівнях сприятливі умови для стабільності, передбачуваності й чесної конкуренції. Цю політику потрібно розробляти і здійснювати так, щоб не тільки залучати приватні інвестиції в розвиток інфраструктури ІКТ, а й забезпечувати виконання зобов’язань щодо універсального обслуговування в тих сферах, де не діють традиційні ринкові механізми;

3) *доступ до інформації і знань*. Полягає у забезпеченні кожному можливості мати доступ до інформації, ідей і знань та робити свій внесок;

4) *нарощування потенціалу, тобто* кожна людина повинна мати можливість опановувати навички і знання, потрібні для розуміння суті інформаційного суспільства та економічних знань, для активної участі в ньому і повномасштабного використання його переваг.

5) *зміцнення довіри й безпеки при використанні ІКТ*. Означає інформаційну безпеку та безпеку мереж, аутентифікацію, захист не-

доторканності приватного життя і прав споживачів, та є передумовою становлення інформаційного суспільства і зростання довіри з боку користувачів ІКТ.

6) *формування сприятливого середовища*, що є важливою умовою існування інформаційного суспільства. Таке середовище має формуватися як на національному, так і на міжнародному рівнях. Воно має забезпечувати:

- верховенство права, прозору, сприятливу конкуренцію, технологічно нейтральну і передбачувану політичну і регламентну базу;
- застосування ІКТ як важливого інструменту належного державного управління;
- забезпечення захисту інтелектуальної власності для заохочення інноваційної діяльності і творчості в інформаційному суспільстві;
- особливу увагу до розроблення і ухвалення міжнародних стандартів;
- керування використанням радіочастотного спектра в інтересах суспільства;
- керування використанням Інтернет на міжнародному рівні, яке охоплює як технічні питання, так і питання державної політики і в якому мають брати участь усі зацікавлені сторони, міжнародні, міжурядові та неурядові організації;

7) *додатки на базі ІКТ: переваги в усіх аспектах життя* – використання і розгортання ІКТ має бути спрямоване на створення переваг у всіх аспектах нашого повсякденного життя. Додатки ІКТ мають бути зручними для користувачів, доступними для всіх, прийнятними з цінового погляду, відповідати місцевим потребам завдяки адаптації до місцевих мов і культур та підтримувати стійкий розвиток;

8) *культурна різноманітність і культурна самобутність, мовна різноманітність*, оскільки це забезпечує збереження загальної спадщини людства, що передбачено відповідними програмними документами ООН;

9) *визнання засобів масової інформації* основною складовою інформаційного суспільства. Підтверджується потреба дотримання свободи преси та свободи інформації, а також їх незалежності, плюралізму й різноманітності;

10) дотримання *етичних аспектів інформаційного суспільства*, які полягають у потребі поважати мир і обстоювати такі основні цін-

ності, як воля, рівність, солідарність, терпимість, колективна відповідальність і дбайливе ставлення до природи;

11) *міжнародна та регіональна співпраця*, що є важливою умовою розбудови інформаційного суспільства, оскільки останнє є глобальним по суті. Основна мета такої співпраці – сприяння подоланню розриву в цифрових технологіях, розширення доступу до ІКТ, створення цифрових можливостей і використання потенціалу ІКТ в інтересах розвитку. Окремо визначено роль Міжнародного союзу електрозв'язку в реалізації основних цілей розбудови інформаційного суспільства.

У розділі С Декларації “До інформаційного суспільства для всіх, заснованому на спільному використанні знань” викладені зобов'язання держав-учасниць ООН щодо зміцнення співпраці з метою реалізації Плану дій та принципів Декларації, періодичного оцінювання ефективності вжиття заходів та координації міжнародних зусиль з розбудови інформаційного суспільства.

Важливим кроком України на шляху до активного залучення нашої держави до процесів розбудови інформаційного суспільства стало прийняття в січні 2007 р. Закону України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки”³⁵. Закон передбачає реалізацію цілей і принципів, сформульованих у Декларації. Викладені в ньому основні засади є концептуальною основою для розроблення завдань розвитку інформаційного суспільства в Україні.

За нормами розділу III Закону, національна політика України щодо розбудови інформаційного суспільства має забезпечувати:

- перехід до пріоритетного науково-технічного та інноваційного розвитку;
- законодавче забезпечення розвитку інформаційного суспільства;
- формування сприятливих економічних умов розвитку інформаційного суспільства;
- розвиток загальнодоступної інформаційної інфраструктури;
- повсюдний доступ до телекомунікаційних послуг та інформаційних ресурсів;
- сприяння збільшенню різноманітності та кількості електронних послуг;

³⁵ Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 9 січня 2007 р. № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102.

- створення загальнодоступних електронних інформаційних ресурсів;
- підготовку людини до роботи в інформаційному суспільстві;
- створення системи мотивацій щодо впровадження і використання ІКТ;
- пріоритетний розвиток науки та культури в інформаційному суспільстві;
- охорону здоров'я в інформаційному суспільстві;
- охорону навколишнього природного середовища;
- захист інформаційної безпеки в інформаційному суспільстві.

Для виконання завдань розвитку інформаційного суспільства Закон передбачає (Розділ IV) створення відповідних організаційно-правових основ, таких як: інституційне, організаційне та ресурсне забезпечення; відповідні об'єднання громадян; механізми інтеграції України у світовий інформаційний простір та механізми реалізації Основних засад розвитку інформаційного суспільства в Україні на 2007–2015 роки.

Хоча самі по собі перелічені вище нормативно-правові акти мають декларативний характер, викладені в них принципи і завдання є основою для розроблення конкретних заходів у межах проведення державної інформаційної політики та окремих планів і програм. Крім того, такі норми мають характер морального зобов'язання публічної влади держави щодо цілей, яких потрібно досягти в рамках розвитку інформаційного суспільства, відбивають офіційну позицію щодо бачення сутності і змісту такого суспільства. Передбачається, що реалізація визначених у цих актах концептуальних засад дасть змогу забезпечити позитивні зміни в життєдіяльності суспільства і людини.

ГЛАВА 2

ПРЕДМЕТ, МЕТОД І СИСТЕМА ІНФОРМАЦІЙНОГО ПРАВА

*Предмет інформаційного права. Метод
інформаційного права. Поняття, система та
джерела інформаційного права. Класифікація
інформації в українському законодавстві.
Поняття та структура інформаційних
правовідносин. Інформаційний простір та
інформаційний суверенітет.*

2. 1. Предмет інформаційного права

Багатоманітність і динаміка інформаційних відносин у сучасному суспільстві є настільки виразними, що навіть немає ще повної визначеності з поняттям самого інформаційного права, якміс мають регулюватися ці відносини. Правові норми з питань регулювання певних груп інформаційних відносин (державна таємниця, інформація для службового користування, діяльність ЗМІ, технічні стандарти телекомунікаційних систем тощо) виникали разом із появою та розвитком відповідних суспільних або технічних явищ.

Специфіку правового регулювання в інформаційній сфері почали детально розглядати лише в 70-ті роки ХХ ст., коли сталися революційні зміни як у кількісних, так і в якісних характеристиках інформаційних відносин, зумовлені технічним та соціальним прогресом людства. Причому іноді подібне правове регулювання чомусь намагалися ідентифікувати з такими “інформаційними” науками, як інформатика і кібернетика. Навіть обстоювалося існування специфічної галузі “правова інформатика” як “міждисциплінарної галузі знання про закономірності й особливості інформаційних процесів у сфері юридичної діяльності, про автоматизацію та використання автоматизованих інформаційних систем”³⁶.

Подібні міркування заслуговують на увагу, проте нагадують спробу штучно поєднати суспільну та природничу галузь науки, що, з од-

³⁶ Гаврилов О. А. Курс правової інформатики. – М. : Изд-во НОРМА, 2000. – С. 66.

ного боку, є надто вузьким розумінням проблем взаємодії правових норм та інформаційних відносин у суспільстві, а з другого – є дуже ускладненим варіантом суто практичної проблеми використання комп'ютерних технологій у державному управлінні. Хоча не слід забувати про фатальне відставання колишнього СРСР у сфері інформатизації суспільства від США та країн Західної Європи. На думку багатьох дослідників, таке відставання було зумовлене не тільки технічними факторами, а й несприятливими для розвитку інформаційних відносин авторитарною політичною системою та закритим типом суспільства³⁷. Саме тому інформатизація в колишньому СРСР могли застосовувати лише у науці, на виробництві (що не потребувало правового регулювання) або у державному управлінні.

Проте в 1978 р. А. Б. Венгеров порушив питання про виділення самостійної галузі інформаційного права³⁸. Згодом він обґрунтував також виділення нової галузі інформаційного права, віднісши її до галузей права, які *поки що* виокремлюються за своїм суспільно значущим предметом, а метод регулювання може напрацьовуватися³⁹.

Демократичні процеси в колишньому СРСР наприкінці 90-х років минулого століття, здобуття незалежності колишніми радянськими республіками, ринкові перетворення сприяли формуванню інформаційних відносин нового типу. Власне новими ці відносини стали лише для пострадянських держав, оскільки в розвинених західних країнах існували вже давно. Але навіть декларативних заяв про бажання приєднатися до загальносвітових інформаційних процесів було достатньо для широкого обговорення проблеми становлення та підвищення ролі галузі інформаційного права.

Наприклад, у 1995 р., Ю. А. Тихомиров, розглядаючи проблему інформаційного права, виділив *комплекс специфічних правових питань*, що регулюються в рамках цієї галузі, що на його думку, дає змогу розглядати інформаційне право як нову комплексну галузь, що є частиною публічного права⁴⁰. А вже в 2002 р. В. А. Копилов без будь-яких сумнівів характеризує інформаційне право як нову комплексну галузь, що є системою соціальних норм і відносин, які охороняються державою і виникають в інформаційній сфері – сфері виробництва,

³⁷ Кастельс М. Информационная эпоха: экономика, общество, культура: Пер. с англ. под науч. ред. О. И. Шкаратана. – М.: ГУ ВШЭ, 2000. – С. 435–455.

³⁸ Венгеров А. Б. Право и информация в условиях автоматизации управления. – М., 1978.

³⁹ Венгеров А. Б. Теория государства и права. – М., 1999. – С. 381.

⁴⁰ Тихомиров Ю. А. Публичное право. – М., 1995. – С. 339.

перевтілення та споживання інформації, а також визначає на предмет правового регулювання інформаційного права – “інформаційні відносини, тобто відносини, що виникають при здійсненні інформаційних процесів – процесів виробництва, збирання, обробки, накопичення, зберігання, пошуку, передачі, розповсюдження та споживання інформації”⁴¹.

Однак, цей підхід до визначення предмета інформаційного права викликає більше запитань, ніж дає відповідей. Адже, як уже зазначалося, людина є істотою соціальною, і будь-яка сфера її діяльності пов’язана з передаванням інформації, тобто з інформаційними відносинами⁴². Наприклад, процес збирання доказів по кримінальній справі можна розглядати як процес збирання інформації, який має регулюватися нормами інформаційного права, хоча насправді цей процес регулюється нормами кримінально-процесуального права. І таких прикладів можна навести безліч. Тобто наведено вище визначення предмета інформаційного права є абсолютно некоректним, оскільки фактично не залишає місця для існування будь-яких інших галузей права, крім інформаційного.

Для розуміння цієї суперечності потрібно більш чітко визначити предмет інформаційного права. З одного боку, ця потреба спонукає багатьох дослідників до запровадження різних синтетичних категорій на кшталт “предметна сфера інформаційного права” або “кілька комплексів суспільних відносин, які цементуються єдністю об’єкта – інформацією”, а з другого – створює тенденцію до обмеження кола суспільних відносин, які охоплюються цими категоріями. Зокрема, до цих категорій належать:

- а) всі види діяльності, пов’язані з інформаційним ресурсом як об’єктом діяльності (продукту інтелектуальної, виробничої, будь-якої іншої соціальної діяльності);
- б) управління в галузі відносин, пов’язаних з певним інформаційним ресурсом та окремими видами роботи з інформацією;
- в) використання нових технологій роботи з інформацією – формування і забезпечення сумісності інформаційних систем і систем комунікацій в інформаційних системах та мережах;
- г) забезпечення безпеки у сфері інформації та інформатизації;

⁴¹ Копылов В. А. Информационное право. – 2-е изд., перераб. и доп. – М.: Юрист, 2002. – С. 86–87.

⁴² Див. доклад.: Кормич Б. А. Інформація як категорія інформаційного права // Актуальні проблеми держави і права: Зб. наук. праць. – Вип. 16. – Одеса: Юрид. літ-ра, 2002. – С. 367–374.

д) реалізація юридичної відповідальності в галузі інформації, інформатизації, телекомунікацій⁴³.

Проте, подібна конструкція так само не дає уявлення про предмет інформаційного права, оскільки під дефініціями “всі види діяльності, пов’язані з інформаційним ресурсом” та “певні види діяльності з інформацією” можна розуміти будь-що. А аргументація побудована на тезі про незавершений процес формування галузі інформаційного права може викликати лише пропозицію зачекати з виділенням цієї галузі до завершення її формування.

Значною помилкою при визначенні предмета інформаційного права є розгляд у цій якості виключно суспільних відносин, адже предмет правового регулювання має набагато складнішу структуру, яка охоплює: суб’єкти, об’єкти регулювання суспільних відносин та соціальні факти, з якими пов’язане виникнення відповідних відносин⁴⁴.

Крім того, для чіткого обмеження предметної сфери інформаційного права недоцільно розглядати як предмет регулювання будь-які суспільні відносини, що виникають з приводу інформації чи інформаційних процесів, адже інформація як така є складовою будь-якого типу суспільних відносин. Для інформаційного права важливі лише суспільні відносини, що визначають *параметри і характеристики інформаційних процесів*, тобто насамперед їх види, форми, засоби, й вже потім змістовне наповнення, яке не завжди має значення для правового регулювання. Наприклад, Закон України “Про інформацію”⁴⁵ (ст. 1) визначає останню як “документовані або публічно оголошені відомості”, тим самим акцентуючи увагу саме на формальних ознаках. Навіть коли йдеться про специфічні види інформації, наприклад такі як державна таємниця, конфіденційна інформація або інформація (інформаційна продукція), що містить пропаганду війни, насильства, жорстокості тощо, то правові норми, якими регулюються режими суспільного обігу цієї інформації, орієнтовані не на конкретний її зміст, а на мету та наслідки її розповсюдження, тобто на зовнішні характеристики пов’язаних із нею інформаційних процесів. Крім того, з огляду на зазначеної норми ст. 1 Закону України “Про інформацію” серед безлічі інформаційних процесів слід виділити два *базових*, які роблять виникаючі з їх приводу суспільні відносини предме-

⁴³ Див.: Бачило І. Л., Лопатин В. Н., Федотов М. А. Информационное право / Под ред. Б. Н. Топорнина. – СПб: Юрид. центр Пресс, 2001 – с. 97–98.

⁴⁴ Теория государства и права /Под ред. Бабаева В. К. – М. : ЮристЪ, 1999. – С. 391.

⁴⁵ Закон України “Про інформацію” від 2 жовтня 1992 р. // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

том правового регулювання, це – *процеси документування та публічного оголошення (розповсюдження) інформації*.

Іншим елементом предмета інформаційного права є правовий статус суб'єктів інформаційних процесів, причому не в загальноправовому розумінні, а такий, що визначає права, обов'язки та взаємозв'язки цих суб'єктів щодо визначення або дотримання параметрів інформаційних процесів, доступу та прав на інформацію тощо. Велике значення специфіки правового статусу суб'єктів для формування інформаційного права підкреслює В. А. Копилов, висловлюючи думку про те, що основу інформаційного права, його юридичний базис становлять *інформаційні права і свободи*, забезпечення гарантій яких є основною метою цієї нової галузі права⁴⁶. Конкретніше, ці права і свободи слід розглядати як невід'ємну складову правового статусу людини як суб'єкта інформаційних правовідносин. До того ж, саме з'ясування на міжнародному та національному рівнях низки “інформаційних прав” багато в чому посприяло розвитку багатьох типів інформаційних відносин і процесів.

Стосовно третього елемента предмета правового регулювання найбільш вдалою є висловлена свого часу В. Д. Сорокіним теза щодо “поведінки поза правовідносинами”, за якої дії суб'єктів регулюються системою заборон без виникнення правових відносин. Регулювання цього елемента досягають забезпеченням належного виконання вимог заборонних правових норм, тобто пасивної поведінки щодо дій, які держава вважає як правопорушеннями⁴⁷. Саме характер заборон мають механізми захисту від неправомірного інформаційного втручання від таємниці приватного життя і закінчуючи заборонами на пропаганду війни, насильства, расової дискримінації тощо. А формування правового регулювання роботи автоматизованих інформаційних систем, зокрема мережі Інтернет, взагалі почалося з вироблення їх користувачами специфічних моральних норм, які дістали назву “мережевого етикету”, котрі саме становили систему заборон на певні некоректні дії щодо інших користувачів.

Отже, предмет інформаційного права можна визначити як *суспільні відносини, що виникають з приводу встановлення режимів та форм обігу інформації, реалізації інформаційних прав і правового статусу суб'єктів інформаційних процесів і формування їх правомірної поведінки і зв'язків*.

⁴⁶ Копылов В. А. Информационное право. – 2-е изд., перераб. и доп. – М. : Юрист, 2002. – С. 88.

⁴⁷ Сорокин В. Д. Метод правового регулирования. Теоретические проблемы. – М. : Юрид. лит. – 1976 – С. 79.

2. 2. Метод інформаційного права.

Серед науковців існують значні розбіжності у визначенні методу інформаційного права, оскільки метод конструюється зазвичай з урахуванням особливостей предмета правового регулювання. Тому наводиться переважно приклад так званого “комплексного методу” який, за різними поглядами, може бути собою складною конструкцією, що поєднує в собі два (імперативний та диспозитивний) і більше методів правового регулювання інших галузей права. Так, І. Л. Бачило, характеризуючи цю проблему, стверджує, що “в системі інформаційного права реалізуються методи конституційного, адміністративного, цивільного, кримінального права, процесуальних норм цих галузей, в ньому використовуються методи міжнародного публічного і приватного права, зберігають певну ступінь впливу заходи звичаєвого права та ділових навичок”⁴⁸. І знову, як і в ситуації з предметом інформаційного права, таке визначення методу дає підстави відносити до інформаційного права будь-що й, одночасно нічого, не даючи чіткого уявлення про цю галузь.

У визначенні методу правового регулювання інформаційного права ключовим має бути розуміння того, що специфіка цього методу багато в чому зумовлена характером суспільних відносин, які підлягають регулюванню тією чи іншою сукупністю правових норм. Так, П. М. Рабінович, визначаючи галузь права як систему юридичних норм, що регулюють певну сферу суспільних відносин, специфічним методом правового регулювання, підкреслює нерівноцінність цих двох елементів, вважає, що “первинним, визначальним серед них є предмет правового регулювання, який... веде за собою метод”⁴⁹.

Але ж характеризуючи метод інформаційного права, потрібно відійти від традиційних диспозитивного та імперативного методів правового регулювання чи їх комбінації. Оскільки в такому разі неможливо зробити ніяких висновків, крім констатації тісного зв'язку інформаційного права з іншими галузями права та використання ним норм і методів останніх.

Правове регулювання, маючи складну структуру складається з кількох базових елементів, “цеглин”, комбінація яких і дає специфічні методи окремих галузей права. Адже якщо головне значення пред-

⁴⁸ Бачило І. Л. Информационное право. Основы практической информатики. – М., 2001. – С. 52.

⁴⁹ Рабінович П. М. Основы загалльної теорії права та держави. – К. – 1994. – С. 95.

мета зумовлює юридичний характер засобів впливу на предмет у цілому і його складові елементи, а відповідно і правову природу методу, то системна структура предмета правового регулювання з такою самою неминучістю визначає відповідно системну структуру самого методу правового регулювання”⁵⁰.

Характеризуючи базові елементи правового регулювання, С. С. Алексєєв виділив з усієї маси дозволів і заборон загальні дозволи й загальні заборони, які є особливими режимами правового регулювання і “виражають існування двох головних типів (порядків) правового регулювання”⁵¹. Поряд із дозволами та заборонами діє і третій тип правового регулювання, що ґрунтується на системі позитивних зобов’язань. Проте такі зобов’язання, на думку Алексєєва, якісно відрізняються від двох головних типів правового регулювання, побудованих на дозволах і заборонах, оскільки *не мають зв’язку із суб’єктивними правами*⁵².

Існує чотири специфічних види правового регулювання суспільного обігу інформації: закритий, обмежений, відкритий і вільний⁵³. Параметри інформаційних процесів, що відбуваються в рамках *закритого обігу*, визначаються державними органами на основі владних приписів; параметри *відкритого обігу* – безпосередньо суб’єктами інформаційних процесів на основі реалізації їхніх прав на відповідну інформацію. *Обмежений обіг* – це комбінація двох перших видів обігу (наприклад, параметри розповсюдження інформаційної продукції еротичного характеру, які також визначає держава, – віковий ценз, та суб’єкти інформаційних відносин – умови передачі інформації); *вільний обіг*, безпосереднє правове регулювання якого не здійснюється, представляє якраз і є згаданою вище “поведінкою поза правовідносинами”.

Та попри всі відмінності між різними видами суспільного обігу інформації в основі їх правового регулювання лежать однакові принципи і способи, що дає змогу визначати основні характеристики методу інформаційного права.

У методі інформаційного права є зокрема, головний такий базовий елемент, як загальні дозволи. Раніше вже зазначалося визначаль-

⁵⁰ Сорокин В. Д. Метод правового регулирования. Теоретические проблемы. – М. : Юридическая литература, 1976 – С. 102.

⁵¹ Алексєєв С. С. Общие дозволения и общие запреты в советском праве. – М. : Юрид. лит. – 1989 – С. 104.

⁵² Там само. – С. 105 – 106.

⁵³ Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України. – Оdesa: Юрид. літ. – 2003 – С. 338.

не значення для інформаційного права загальноновизнаних прав і свобод людини в галузі інформації. У загальному вигляді ці права можна визначити через принцип “свободи інформації”, який є загальним дозволом на вільне збирання, зберігання, оброблення та розповсюдження інформації. Так, згідно зі ст. 5 Закону України “Про інформацію”, до основних принципів інформаційних відносин належать: гарантованість права на інформацію та відкритість, доступність інформації і свобода її обміну.

Для ефективного практичного застосування загальні дозволи збалансовано та врегульовано за допомогою системи заборон вже як загального, так і приватного характеру (обмеження, вилучення, тощо), які є другим за значенням елементом методу інформаційного права. Слід зазначити, що заборони не лише обмежують інформаційні права і свободи, а й виступають одним із засобів реалізації останніх. Наприклад, забезпечення передбаченої ч. 2 ст. 32 Конституції України таємниці приватного життя, юридично реалізовано саме через заборону збирати, зберігати, використовувати та поширювати конфіденційну інформацію про особу без її згоди.

Проте найбільш характерною ознакою методу інформаційного права є обмежене використання позитивних зобов'язань. Це можна прояснити двома основними причинами. По-перше, це брак зв'язку позитивних зобов'язань із суб'єктивними правами, які становлять базис інформаційного права. По-друге, це загальна спрямованість розвитку інформаційного законодавства, яка характеризується відмовою від використання прямих приписів. Наприклад, норма ч. 3. ст. 15 Конституції України передбачає заборону цензури, тобто заборону прямого втручання держави в інформаційні процеси.

Отже, можна визначити *метод інформаційного права як специфічний спосіб правового впливу на характеристики інформаційних процесів, базисом якого є система загальних дозволів і який збалансовується за допомогою системи заборон загального і приватного характеру та обмежено використовує позитивні зобов'язання.*

2. 3. Поняття, система і джерела інформаційного права

У визначенні місця інформаційного права в системі права слід враховувати кілька основних позицій.

По-перше, зважаючи на специфіку предмета й метод інформаційного права, можна чітко визначити його відмінність від деяких інших галузей права, до складу яких зазвичай вводилися інформаційні норми. Йдеться про найбільш поширені погляди на зв'язок інформаційного права або з адміністративним⁵⁴, або із цивільним правом⁵⁵.

На відміну від адміністративного права, до предмет якого охоплює сукупність суспільних відносин, які виникають у процесі *організації і функціонування* (виділено нами – *Б. К.*) органів державного управління і здійснення ними заходів адміністративно-правового примусу і притягнення до адміністративної відповідальності⁵⁶, до предмету інформаційного права визначення організаційної структури суб'єктів інформаційних процесів *не входить*. Крім того, в інформаційному праві основу методу правого регулювання становлять загальні дозволи, на відміну від методу адміністративного права, який ґрунтується на владних приписах.

Щодо зв'язків *інформаційного права з цивільним*, то останнє передбачає за загальним правилом абсолютну рівність суб'єктів, тоді як в інформаційному праві від початку закладена різноплановість правового статусу суб'єктів (фізичних і юридичних осіб, органів державного управління, посадових осіб, осіб, які мають допуск до конфіденційної інформації, тощо). Крім того, в регулюванні суспільного обігу деяких видів інформації (державна таємниця, конфіденційна інформація, що перебуває у власності держави тощо) або регулювання певних інформаційних процесів (діяльність систем спеціального та урядового зв'язку) для інформаційного права характерні владні відносини та відносини підпорядкування, які неможливі в цивільному праві.

Отже, можна характеризувати *інформаційне право як виокремлену групу правових норм, якими регулюються суспільні відносини, що виникають з приводу встановлення режимів та параметрів суспільного обігу інформації, правового статусу, поведінки та зв'язків суб'єктів інформаційних процесів*.

⁵⁴ Бачило І. Л. Информационное право. Основы практической информатики. – М., 2001 – С. 55.

⁵⁵ Гостев И. М. Информационное право в России // Конфидент. – 2000 – № 1 – 2. январь – апрель. – С. 15 – 22.

⁵⁶ Адміністративне право України / Під. ред. С. Ківалова. – Одеса: Юрид. літ. – 2003. – С. 8.

Другим важливим питанням є статус *інформаційного права*. Існує думка про те, що інформаційне право є комплексною галуззю. Однак зазначимо, що вирішення цього питання багато в чому залежить від доктринальних підходів, оскільки в теорії права спостерігаються як визнання, так і цілковите заперечення існування так званих комплексних галузей. Назагал розвиток поглядів на предмет і метод інформаційного права свідчать, що теоретичних перешкод для визнання інформаційного права самостійною галуззю немає. Але слід враховувати, що нині правове регулювання питань щодо предмета інформаційного права офіційно поєднує конституційне, адміністративне та цивільне право. Разом з тим уже сьогодні можна говорити про інформаційне право як про галузь законодавства, що об'єднує нормативно-правовий матеріал, яким регулюється відносно відособлена група суспільних відносин, застосовуючи при цьому специфічні методи регулювання.

Важливим чинником, є також *динамічність* інформаційного права, формування якого відбувалося завдяки таким чинникам, як: посилення ролі прав і свобод людини та громадянина в інформаційній діяльності суспільства і держави, розвиток інформаційних технологій, офіційне визнання процесів глобалізації та формування інформаційного суспільства і пов'язаних з ними змін у виробничій, політичній та соціальній сферах суспільного життя. Отже, визначально зростає роль правового регулювання інформаційних відносин та зацікавленість у формуванні стабільного й самодостатнього правового регулювання в цій сфері.

Інформаційне право, як і будь-яка галузь права, має свою внутрішню структуру – систему. Основними структурними елементами галузі права є норми права та інститути права. В межах інститутів права іноді виділяють менші утворення – субінститути.

Відмінність інформаційно-правових норм від норм в інших галузях права в тому, що вони регулюють відносини, які виникають в інформаційній сфері у зв'язку з реалізацією інформаційних прав і свобод та здійсненням інформаційних процесів при послугоуванні інформацією. Залежно від виду і форми подання інформації, суб'єктів, що діють в інформаційній сфері, особливостей їх поведінки інформаційно-правові норми поділяють на імперативні й диспозитивні⁵⁷.

⁵⁷ Копилов В. А. Информационное право. – М. : Юрист, 2002 – с. 122.

Ключовими для визначення сутності інформаційного права, безперечно, є *диспозитивні норми*. Так, визначаючи місце того чи іншого типу правових норм у системі інформаційного права, слід враховувати, що в цій галузі виступають як інформаційні права і свободи людини, зокрема, свобода думки і слова, яка, згідно зі ст. 34 Конституції України, полягає в тому, що “кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір”⁵⁸. У більш широкому розумінні такою основою виступає “право на інформацію”, яке за ст. 9 Закону України “Про інформацію” визначає, що “всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій”⁵⁹.

Установлення певної категорії прав і свобод суб’єктів правових відносин означає насамперед визначену законодавством можливість скористатися (реалізувати) право. А така можливість вибору відповідного типу поведінки характерна саме для диспозитивного типу регулювання.

Таким чином, саме *диспозитивні норми* формують підвалини інформаційного права, встановлюючи загальні основні дозволи, які, зокрема, регулюють відносини щодо встановлення основних прав і свобод людини, правового статусу інших суб’єктів інформаційного права, основних принципів інформаційного права, серед яких головним є забезпечення свободи збирання та поширення інформації.

Існуючі в інформаційному праві імперативні норми, у свою чергу, залежно від регулятивних функцій, які вони виконують, можна поділити на: *норми-принципи, норми-декларації, норми-заборони та норми-приписи*.

Однією із особливостей сучасного інформаційного права є відносно широке порівняно з іншими галузями використання саме *норм-принципів та норм-декларацій*. Адже важливим аспектом інформаційного права є забезпечення інформатизації та розбудови інформа-

⁵⁸ Конституція України. Прийнята Верховною Радою України 28 червня 1996 року // Відомості Верховної Ради України. – 1996. – № 30 – Ст. 141.

⁵⁹ Про інформацію: Закон України від 2 жовтня 1992 р. // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650

ційного суспільства. Отже, в інформаційному-праві за допомогою норм-принципів та норм-декларацій не лише визначаються звичайні для будь-якої галузі принципи, а й установлюються основи державної інформаційної політики, визначають перспективні плани та програми розвитку. Наприклад, такий нормативно-правовий акт, як Закон України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки”⁶⁰, практично повністю складається із норм-принципів та декларацій.

Норми-заборони в інформаційному праві виконують кілька функцій. По-перше, вони збалансовують установлену диспозитивними нормами систему загальних дозволів, формуючи систему винятків щодо права на інформацію – заборони розголошення, заборони збирання, заборони розповсюдження з метою охорони прав і законних інтересів третіх осіб – суб’єктів інформаційних процесів, інтересів держави та суспільства тощо. Наприклад, ст. 49 Закону України “Про інформацію” установлює неприпустимість зловживання правом на інформацію, встановлюючи обмеження щодо вільного розповсюдження та розголошення деяких видів інформації.

По-друге, *норми-заборони* деколи слугують гарантією реалізації права на інформацію та захисту прав і свобод людини у сфері інформації. Так, норма ч. 3 ст. 15 Конституції України визначає, що “цензура заборонена”, *норми* ст. 32 Конституції України забороняють втручання в особисте життя та збирання, зберігання, використання й поширення конфіденційної інформації про особу без її згоди.

Нарешті, *норми-приписи* в інформаційному праві зазвичай використовують для створення механізмів, визначення конкретних способів та засобів реалізації прав суб’єктів інформаційних відносин. *Норми-приписи* в інформаційному праві, зокрема, визначають: компетенцію органів публічної влади щодо регулювання інформаційних відносин, правові режими інформації та інформаційних ресурсів, стандарти і правила інформаційної діяльності та ін. Наприклад, ст. 40 Конституції України визначає зобов’язання органів державної влади, органів місцевого самоврядування та посадових і службових осіб цих органів, розглядати направлені до них звернення громадян і давати обґрунтовані відповіді у встановлений законом строк. *Норми* ст. 13 і 14 Закону України “Про Національну раду України з питань телеба-

⁶⁰ Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України від 9 січня 2007 р. № 537-V // Відомості Верховної Ради України – 2007. – № 12. – Ст. 102.

чення і радіомовлення” передбачають, контрольні й регуляторні повноваження Нацради щодо телебачення і радіомовлення.

Норми інформаційного права, як і норми більшості галузей права також можна поділити на матеріальні і процесуальні. Якщо порівнювати їх співвідношення, у системі інформаційного права, то більшість становлять *матеріальні норми* інформаційного права, якими регламентуються права, обов’язки, компетенція суб’єктів, правила та стандарти здійснення інформаційної діяльності, правові режими тощо.

Процесуальні норми інформаційного права є нечисленними і мають переважно характер процедурних норм, визначаючи певну послідовність дій суб’єктів певних видів інформаційних відносин. До прикладу, у Законі України “Про державну таємницю” ст. 10 визначає порядок віднесення інформації до державної таємниці, а ст. 15 порядок засекречування та розсекречування матеріальних носіїв інформації.

Щодо ролі процесуальних норм в інформаційному праві варто зазначити, що в цій галузі для реалізації матеріальних норм широко використовуються процесуальні норми інших галузей права. Зокрема частина норм, що визначають право на інформацію, правила здійснення інформаційної діяльності тощо, реалізовується в процесі діяльності органів виконавчої влади. Це, наприклад стосується надання інформації на запити, реєстрації та ліцензування засобів масової інформації тощо. Отже, виникає добре відома в адміністративному праві ситуація, коли “в ході реалізації адміністративно-процесуальних норм обслуговуються норми не лише матеріального адміністративного права, але й норми інших матеріальних галузей права”⁶¹. Причому в межах управлінської діяльності органів виконавчої влади та місцевого самоврядування можливе застосування не тільки матеріальних, а й процесуальних норм різних галузей права.

Важливим елементом реалізації низки матеріальних норм інформаційного права є *судовий захист*. Наприклад, ст. 55 Конституції визначає судовий захист прав і свобод людини і громадянина. Широко відомою є розглянута Конституційним Судом України так звана “Справа К. Г. Устименко” щодо визначення обсягу та порядку охорони конфіденційної інформації про особу. У цьому аспекті матеріальні норми інформаційного права реалізуються в межах процесуальних галузей – цивільного, адміністративного, господарського процесу, процедур Конституційного Суду тощо.

⁶¹ Бандурка А. М. , Тищенко Н. М. Адміністративний процес. – К. , 2001 – С. 10

За своєю структурою система інформаційного права поділяється дві частини – загальну й особливу.

До *загальної частини* інформаційного права належать правові норми, що визначають основи цієї галузі:

- загальні поняття та принципи інформаційного права;
- предмет і метод інформаційного права;
- класифікація інформації.

Крім того, до загальної частини інформаційного права належать кілька універсальних інститутів, що об'єднують близькі за змістом правові норми, що визначають ключові питання інформаційних відносин:

- інститут інформаційних прав і свобод людини і громадянина;
- інститут інформаційної безпеки;
- інститут правового режиму інформації
- інститут правового режиму інформаційних ресурсів;
- інститут правових основ розбудови інформаційного суспільства.

Особлива частина інформаційного права охоплює інститутів, в межах яких реалізуються основні права та обов'язки суб'єктів інформаційних відносин, що ґрунтуються на нормах загальної частини. До інститутів особливої частини інформаційного права, зокрема, можна віднести:

- інститут державної таємниці;
- інститут конфіденційної інформації;
- інститут захисту інформації;
- інститут інформаційного забезпечення публічної влади;
- інститут телекомунікацій;
- інститут мережі Інтернет;
- інститут вільної преси;
- інститут електронних засобів масової інформації.

Цей перелік, звісно не є вичерпним, але ілюструє основні групи правових норм, що різняться особливостями реалізації регулятивного впливу та певною відокремленістю та суспільним значенням предмета правового регулювання. Крім того, більшість із названих інститутів дістають своє формальне вираження в певних нормативно-правових актах, що регулюють відповідний вид суспільних відносин.

Під джерелами інформаційного права слід розуміти зовнішні форми вираження норм інформаційного права, за допомогою яких відбуваються формування та закріплення цих норм. Система джерел інформаційного права є аналогічною відповідним системам інших га-

лузей вітчизняного законодавства. Таким чином, система джерел інформаційного права представлена як національним законодавством, так і актами міжнародного права.

Міжнародно-правова складова джерел інформаційного права насамперед представлена багатосторонніми (більшою мірою) та двосторонніми міжнародними договорами, рішеннями міжнародних міжурядових організацій з питань, що стосуються інформаційної сфери (ООН, Рада Європи, ОБСЄ, Міжнародний союз електрозв'язку, СОТ тощо) та іншими джерелами міжнародного права, визнаними ст. 38 Статуту Міжнародного Суду ООН. Ці джерела визначають, зокрема:

- стандарти прав і свобод людини і громадянина у сфері інформації та окремі аспекти реалізації цих прав;
- міжнародну співпрацю щодо інформатизації та розбудови інформаційного суспільства;
- міжнародне регулювання питань зв'язку й телекомунікацій;
- стандарти і співпрацю у боротьбі з правопорушеннями з використанням ІКТ.
- питання міждержавного перебування інформації з обмеженим доступом (на підставі двосторонніх угод).

Національними джерелами інформаційного права є:

- Конституція України (зокрема норми, що визначають права і свободи людини у сфері інформації, захист інформаційної безпеки, загальні принципи діяльності публічної влади);
- рішення Конституційного Суду України, що тлумачать відповідні норми конституції та законодавства;
- законодавчі акти з питань регулювання інформаційних відносин;
- акти Президента України, Кабінету Міністрів України;
- акти міністерств і відомств, галузеві та локальні нормативно-правові акти.

Слід відзначити, що нині в Україні діє близько 30 законів і понад 400 актів Президента та Кабінету Міністрів України, що регулюють суспільні відносини в галузі інформації. Це без врахування таких джерел, як нормативно-правові акти Міністерства транспорту та зв'язку, Міністерства освіти і науки, Міністерства культури і мистецтв, Міністерства внутрішніх справ, Служби безпеки України, Національної комісії з регулювання зв'язку, Національної Ради України з телебачення і радіомовлення, Держкомітету з телебачення і радіомовлення,

Держкомітету архівів, Держкомітету статистики, Адміністрації служби спеціального зв'язку та захисту інформації України та внутрішньогалузеві акти інших міністерств та відомств. Таким чином, нині в Україні сформувалася широка й розгалужена система джерел, що становлять інформаційне законодавство.

2. 4. Класифікація інформації в законодавстві України.

Питання класифікації інформації є важливим для визначення типу правового регулювання, що стосуються суспільних відносин пов'язаних із цією інформацією.

В українському законодавстві є кілька підстав для класифікації інформації залежно від режиму доступу, галузі та виду інформації.

Згідно зі статтями 28–30 Закону України “Про інформацію”⁶², залежно від *режиму доступу* інформація поділяється на вільну та з обмеженим доступом. Інформація з обмеженим доступом, у свою чергу, поділяється на таємну та конфіденційну.

Іншою підставою для класифікації є *галузі інформації*.

Згідно зі ст. 17 Закону України “Про інформацію” визначають, галузями інформації є сукупність документованих або публічно оголошених відомостей про відносно самостійні сфери життя і діяльності суспільства та держави. Основними галузями інформації є такі:

- політична,
- економічна,
- духовна,
- науково-технічна,
- соціальна,
- екологічна,
- міжнародна.

Найбільш розгалуженою і деталізованою є визначена нормами статей 18–25 Закону України “Про інформацію” класифікація інформації за її видами:

- статистична інформація;
- адміністративна інформація (дані);
- масова інформація;

⁶² Закон України “Про інформацію” від 2 жовтня 1992 р. // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

- інформація про діяльність державних органів влади та органів місцевого самоврядування;
- правова інформація;
- інформація про особу;
- інформація довідково-енциклопедичного характеру;
- соціологічна інформація.

Статистична інформація (ст. 19 Закону України “Про інформацію”) – це офіційна документована державна інформація, яка дає кількісну характеристику масових явищ та процесів, що відбуваються в економічній, соціальній, культурній та інших сферах життя. Більш детально питання статистичної інформації регламентуються Законом України “Про державну статистику”. За ст. 6 цього Закону до статистичної інформації належать:

Первинні дані – інформація про кількісних та якісних характеристик явищ і процесів, яка подана респондентами під час статистичних спостережень.

Статистичні дані – інформація, отримана на підставі проведених статистичних спостережень, опрацьована і подана у формалізованому вигляді відповідно до загальноприйнятих принципів та методології.

Зведена знеособлена статистична інформація (дані) – статистичні дані, що є результатом зведення та групування первинних даних при забезпеченні їх знеособленості.

Аналітичні матеріали – відомості, підготовлені на підставі зазначених вище даних.

До статистичної інформації також належать дані, підготовлені на підставі адміністративних даних, отриманих Національним банком України та спеціально уповноваженими органами державної влади відповідно до їх компетенції: *банківська і фінансова статистика, статистика платіжного балансу, митна статистика*.

Важливим аспектом правового регулювання питань статистичної інформації є надання первинним даним статусу конфіденційної інформації та заборона поширення статистичної інформації, на підставі якої можна визначити конфіденційну статистичну інформацію про конкретного респондента (ст. 21, 22 Закону України “Про державну статистику”). Крім того, за загальним правилом статистичні та первинні дані перебувають у державній власності (ст. 23).

Проте забезпечується відкритий доступ зацікавлених осіб до знеособленої статистичної інформації та аналітичних матеріалів через

систематичну відкриту публікацію або надання можливості ознайомлення з нею.

Адміністративна інформація (дані) (ст. 19-1 Закону України “Про інформацію”, ст. 1 Закону України “Про державну статистику”) – це дані, отримані на підставі спостережень, проведених органами державної влади (за винятком органів державної статистики), органами місцевого самоврядування та іншими юридичними особами відповідно до законодавства та з метою виконання адміністративних обов’язків і завдань, віднесених до їх компетенції. Ця інформація представлена у вигляді офіційних документованих даних, які, зокрема, охоплюють усі інші, крім статистики, форми державної звітності та які збирають, використовують, поширюють та зберігають відповідно до законодавства України.

Адміністративні дані про конкретних респондентів мають статус конфіденційної інформації (ст. 21 Закону України “Про державну статистику”).

Масовою (ст. 20 Закону України “Про інформацію”) є публічно поширювана друкована та аудіовізуальна інформація.

Засобами поширення масової інформації є:

– друковані засоби масової інформації – періодичні друковані видання (газети, журнали, бюлетені тощо) і разові видання з визначеним тиражем;

– аудіовізуальні засоби масової інформації – радіомовлення, телебачення, кіно, звукозапис, відеозапис тощо.

Щодо останніх Закон України “Про телебачення і радіомовлення” окремо виділяє такий тип масової інформації, як *аудіовізуальна інформація*, що є зоровою інформацією, що супроводжується звуком⁶³.

Особливості розповсюдження окремих видів масової інформації, так само як і порядок створення та функціонування засобів масової інформації визначаються окремими нормативно-правовими актами: Законами “Про друковані засоби масової інформації (пресу) в Україні”, “Про телебачення і радіомовлення”, “Про інформаційні агентства”, “Про кінематографію”.

Офіційна інформація державних органів та органів місцевого самоврядування (ст. 21 Закону України “Про інформацію”, ст. 1 Закону “Про порядок висвітлення діяльності органів державної влади та ор-

⁶³ Про телебачення і радіомовлення: Закон України від 21 грудня 1993 року // Відомості Верховної Ради України. – 1994. – № 10. – Ст. 43.

ганів місцевого самоврядування в Україні засобами масової інформації”) – офіційна документована інформація, створена в процесі діяльності органів державної влади та органів місцевого самоврядування, яка доводиться до відома населення в порядку, встановленому Конституцією України та законами України.

Основними джерелами офіційної інформації державних органів та органів місцевого самоврядування є нормативно-правові й ненормативні акти, видані цими органами.

Законодавство встановлює низку особливих вимог до розповсюдження цього виду інформації. Так, засобам масової інформації забороняється:

- розрив чи змішування офіційної інформації власними коментарями;
- самостійний переклад офіційної інформації з державної мови на іншу мову.

Крім того, нормами Закону України “Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації” передбачені випадки обов’язкового висвітлення діяльності, передачі й публікації текстів офіційних та екстрених заяв вищих посадових осіб держави з важливих питань державного життя.

Законодавство також визначає способи і шляхи передачі і розповсюдження певного виду інформації, до яких належать:

- публікування в офіційних друкованих виданнях або поширення інформаційними службами відповідних державних органів і організацій;
- публікування в друкованих засобах масової інформації або публічне оголошення через аудіо - та аудіовізуальні засоби масової інформації;
- безпосереднє доведення до зацікавлених осіб (усно, письмово чи іншими способами);
- надання можливості для ознайомлення з архівними матеріалами;
- оголошення під час публічних виступів посадових осіб.

Правова інформація (ст. 24 Закону України “Про інформацію”) є сукупністю документованих або публічно оголошених відомостей про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо.

Серед основних джерел правової інформації (ч. 2 ст. 24 цього Закону) названо Конституцію України, інші законодавчі й підзаконні нормативні правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань.

Важливим джерелом правової інформації є надання громадянам правової допомоги. Відповідно до ч. 2 ст. 59 Конституції, для забезпечення права на захист від обвинувачення та надання правової допомоги при вирішенні справ у судах та інших державних органах в Україні діє адвокатура.

Інформація про особу (ст. 23 Закону України “Про інформацію”) є сукупністю документованих або публічно оголошених відомостей про особу. Основними даними про особу (персональними даними) є: національність, освіта, сімейний стан, релігійність, стан здоров’я, а також адреса, дата і місце народження.

Законом встановлена заборона збирати відомості про особу без її попередньої згоди, за винятком випадків, передбачених законом. Правова регламентація цього виду інформації є важливим елементом захисту одного з ключових громадянських прав права на недоторканість особистого життя, яке визначено нормами ст. 32 та 34 Конституції України⁶⁴. Зокрема, ст. 32 Конституції вводить поняття “конфіденційної інформації про особу”, збирання, зберігання, використання та поширення якої не допускається без згоди цієї особи, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Перелік відомостей, що становлять конфіденційну інформацію про особу, визначено також, у Рішенні Конституційного Суду України у справі про офіційне тлумачення статей 3, 23, 31, 47, 48 Закону України “Про інформацію” та ст. 12 Закону України “Про прокуратуру” (справа К. Г. Устименка)⁶⁵. За цим Рішенням, “до конфіденційної інформації належать свідчення про особу (освіта, сімейний стан, релігійність, стан здоров’я, дата і місце народження, майновий стан та інші персональні дані)”. Слід зазначити, що,

⁶⁴ Конституція України. Прийнята Верховною Радою України 28 червня 1996 року // Відомості Верховної Ради України. – 1996. – №30. – Ст. 141.

⁶⁵ Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України “Про інформацію” та статті 12 Закону України “Про прокуратуру” (справа К. Г. Устименка) від 30 жовтня 1997 року № 5-зп. – Справа № 18/203-97

застосувавши дефініцію “та інші персональні дані”, Конституційний Суд установив можливість розширення переліку конфіденційних даних про особу. Наприклад, за ст. 25 Кодексу законів про працю України⁶⁶ забороняється вимагати в осіб, що приймаються на роботу, відомості про їх партійний стан та національність, походження тощо.

Інформація довідково-енциклопедичного характеру (ст. 24 Закону України “Про інформацію”) є систематизованими, документованими або публічно оголошеними відомостями про суспільне, державне життя та навколишнє природне середовище.

За змістом вона є відкритою, оскільки від початку орієнтована на задоволення потреби суспільства в інформації про навколишній світ, явища та процеси, що відбуваються в ньому. Основними джерелами такої інформації є: енциклопедії, словники, довідники, рекламні повідомлення та оголошення, путівники, картографічні матеріали, а також довідки, які дають уповноважені на те органи державної влади та місцевого самоврядування, об’єднання громадян, організації, їх працівники та автоматизовані інформаційні системи.

Соціологічна інформація (ст. 25 Закону України “Про інформацію”) – документовані або публічно оголошені відомості про ставлення окремих громадян і соціальних груп до суспільних подій та явищ, процесів, фактів. Важлива властивість соціологічної інформації – вона, з одного боку, є одним із інструментів політичного процесу, допомагає визначити політичні орієнтації електорату, що дає змогу формувати стратегію і тактику політичної боротьби, а з другого, розповсюдження соціологічної інформації про рейтинги тих чи інших політичних сил або лідерів, сприйняття суспільством тих чи інших ідей можуть впливати на формування громадської думки.

З цих причин законодавство (наприклад, Закон України “Про вибори народних депутатів України”) встановлює правила та обмеження щодо розповсюдження соціологічної інформації під час проведення виборів до органів публічної влади. Так, засоби масової інформації у разі оприлюднення результатів опитування громадської думки, пов’язаного з виборами депутатів, зобов’язані вказати організацію, що проводила опитування, час його проведення, кількість опитаних, метод збирання інформації, точне формулювання питання, статистичну оцінку можливої похибки.

⁶⁶ Кодекс законів про працю України. – Х.: Одисей, 2001

Забороняється також оприлюднення в день виборів результатів опитування виборців щодо їх волевиявлення під час голосування до його закінчення. А самі способи проведення таких опитувань мають забезпечувати збереження таємниці голосування опитуваного виборця.

Перелік видів інформації, у Законі України “Про інформацію” не є вичерпним. Національне законодавство та ратифіковані Україною міжнародно-правові акти передбачають ще низку інших видів інформації. Так, згідно міжнародними зобов’язаннями України, було встановлено такий вид інформації, як *інформація про стан навколишнього природного середовища (екологічна інформація)* (ст. 25 Закону України “Про охорону навколишнього природного середовища”)⁶⁷ – це будь-яка інформація в письмовій, аудіовізуальній, електронній чи іншій матеріальній формі про:

- стан навколишнього природного середовища або його об’єктів – землі, вод, надр, атмосферного повітря, рослинного і тваринного світу та рівні їх забруднення;
- біологічне різноманіття та його компоненти, у т.ч. генетично видозмінені організми та їх взаємодію із об’єктами навколишнього природного середовища;
- джерела, фактори, матеріали, речовини, продукцію, енергію, фізичні фактори (шум, вібрацію, електромагнітне випромінювання, радіацію), які впливають або можуть вплинути на стан навколишнього природного середовища та здоров’я людей;
- загрозу виникнення і причини надзвичайних екологічних ситуацій, результати ліквідації цих явищ, рекомендації щодо заходів зменшення їх негативного впливу на природні об’єкти та здоров’я людей;
- екологічні прогнози, плани і програми, заходи, в т.ч. адміністративні, державну екологічну політику, законодавство про охорону навколишнього природного середовища;
- витрати, пов’язані зі здійсненням природоохоронних заходів коштом фондів охорони навколишнього природного середовища, інших джерел фінансування, економічний аналіз, проведений у процесі прийняття рішень з питань, що стосуються

⁶⁷ Про внесення змін до деяких законодавчих актів України: Закон України від 28 листопада 2002 р. № 254-IV // Відомості Верховної Ради України. – 2003. – № 4. – Ст. 31.

Основними джерелами такої інформації є дані моніторингу до-вкілля, кадастрів природних ресурсів, реєстри, автоматизовані бази даних, архіви, а також довідки, що видаються уповноваженими на те органами державної влади, органами місцевого самоврядування, громадськими організаціями, окремими посадовими особами.

Науково-технічна інформація (ст. 1 Закону України “Про науково-технічну інформацію”) – “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”⁶⁸.

Реклама (рекламна інформація) (ст. 1 Закону України “Про рекламу”) – інформація про особу чи товар, розповсюджена в будь-якій формі та в будь-який спосіб і призначена сформувати або підтримати обізнаність споживачів реклами та їх інтерес щодо таких особи чи товару⁶⁹.

Інформація в автоматизованих системах (ст. 1 Закону України “Про захист інформації в автоматизованих системах”) – сукупність усіх даних і програм, що використовуються в автоматизованих системах незалежно від засобу їх фізичного та логічного представлення⁷⁰.

Таким чином, законодавча практика майже так само, як і теорія, йде шляхом багатоманітності визначення поняття інформації залежно від сфери та типу інформаційних відносин, що регулюються тим чи іншим нормативно-правовим актом.

2. 5. Поняття і структура інформаційних правовідносин

Участь у суспільних відносинах, врегульованих правом, є засобом реалізації на практиці встановлених законодавством прав і обов’язків. Характеризуючи суспільні відносини, що виникають з приводу інформації, вітчизняне законодавство використовує дефініцію “інформаційні відносини”. Оскільки ці суспільні відносини є

⁶⁸ Про науково-технічну інформацію: Закон України № 3322-XII від 25 червня 1993 р. // Відомості Верховної Ради України. – 1993. – № 33. – Ст. 345.

⁶⁹ Закон України “Про рекламу” від 3 липня 1996 року // Відомості Верховної Ради, 1996. – № 39. – Ст. 181.

⁷⁰ Закон України “Про захист інформації в автоматизованих системах” від 5 липня 1994 р. // Відомості Верховної Ради України. – 2005. – № 26. – Ст. 347.

врегульованими правом, їх можна називати інформаційними правовідносинами.

У найзагальнішому вигляді інформаційні правовідносини – це, “врегульовані інформаційно-правовою нормою інформаційні відносини, сторони яких виступають в якості носіїв взаємних прав та обов’язків, встановлених та гарантованих інформаційно-правовою нормою”⁷¹.

Структурними елементами інформаційних правовідносин виступають:

- об’єкт – те, у зв’язку з чим або з приводу чого виникають правовідносини;
- суб’єкти – учасники правовідносин;
- правовий статус – права, обов’язки та відповідальність суб’єктів;
- поведінка – визначені правовою нормою дії або бездіяльність суб’єктів.

Об’єктом інформаційних відносин, згідно зі ст. 8 Закону України “Про інформацію”, виступає документована або публічно оголошувана інформація про події та явища в галузі політики, економіки, культури, охорони здоров’я, а також у соціальній, екологічній, міжнародній та інших сферах.

Система класифікації *суб’єктів інформаційних правовідносин*, у ній основами їх класифікації виступають такі критерії, як *особа суб’єкта* та *спосіб участі в інформаційних відносинах*. Так, згідно з ч. 1 ст. 7 Закону України “Про інформацію”, суб’єктами інформаційних відносин є:

- громадяни України;
- юридичні особи;
- держава.

Відповідно до ч. 2 ст. 7 цього Закону, суб’єктами інформаційних відносин можуть бути також:

- інші держави;
- громадяни та юридичні особи інших держав;
- міжнародні організації;
- особи без громадянства.

Усі перелічені суб’єкти мають різний правовий статус, який реалізується у процесі інформаційних відносин. Наприклад, іноді участь

⁷¹ Копилов В. А. Информационное право. – М. : Юрист, 2002 – с. 122.

в інформаційних правовідносинах органів публічної влади пов'язана з виконанням ними своїх владних повноважень. Основою правового статусу фізичної особи як учасника інформаційних відносин є його громадянські права і свободи. Особливості правового статусу юридичних осіб багато в чому зумовлені видом інформаційної діяльності, якою вони мають право займатися згідно із законодавством та статутними документами.

Щодо іноземних та міжнародних суб'єктів законодавство передбачає певні обмеження порівняно з аналогічними національними суб'єктами. Такі обмеження, наприклад, стосуються участі у передвиборній агітації, заснування засобів масової інформації та інформаційних агентств, провадження діяльності із захисту інформації, доступу до деяких видів інформації тощо.

За способом участі в інформаційних відносинах, що відповідно зумовлює комплекс їх прав та обов'язків, виокремлюють такі види суб'єктів, як:

- *автор інформації* – особа, що власними силами створює інформацію;
- *власник інформації* – особа, що має права на володіння, користування та розпорядження інформацією;
- *споживач інформації* – особа, що використовує інформацію для задоволення власних інформаційних потреб;
- *поширювач інформації* – особа, що займається діяльністю з розповсюдження, оприлюднення та реалізації інформації;
- *зберігач (охоронець) інформації* – особа, що займається діяльністю із забезпечення належного стану інформації та її матеріальних носіїв і дотримання режиму доступу до інформації.

Визначення конкретного змісту *правового статусу* суб'єктів інформаційних правовідносин є складним з огляду на їх різноплановість та нерівноправність і, як правило, визначається правовими нормами, що регулюють кожний конкретний вид інформаційної діяльності.

Проте існує певний *комплекс універсальних прав, обов'язків та відповідальності* суб'єктів інформаційних відносин, що є загальним для інформаційного права в цілому. Так, суб'єкти інформаційних відносин мають право одержувати (виробляти, добувати), використовувати, поширювати та зберігати інформацію в будь-якій формі з використанням будь-яких засобів, крім випадків, передбачених законом.

Кожний суб'єкт інформаційних відносин для забезпечення його прав, свобод і законних інтересів має право на одержання інформації про:

- діяльність органів державної влади;
- діяльність органів місцевого самоврядування;
- те, що стосується особи.

Основні обов'язки суб'єктів інформаційних відносин є такими:

- поважати інформаційні права інших суб'єктів;
- використовувати інформацію згідно із законом або договором (угодою);
- забезпечувати додержання передбачених законодавством принципів інформаційних відносин;
- забезпечувати доступ до інформації усім споживачам на умовах, передбачених законом або угодою;
- зберігати її в належному стані протягом встановленого терміну і надавати іншим громадянам, юридичним особам або державним органам у передбаченому законом порядку;
- компенсувати шкоду, заподіяну при порушенні законодавства про інформацію.

Поведінка суб'єктів інформаційних правовідносин виявляється у вигляді *інформаційної діяльності*, яка, згідно зі ст. 12 Закону України “Про інформацію”, є сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави.

Законодавство, використовує також дефініцію “*напрями інформаційної діяльності*”: політичний, економічний, соціальний, духовний, екологічний, науково-технічний, міжнародний та ін. Держава гарантує свободу інформаційної діяльності в цих напрямках усім громадянам та юридичним особам у межах їх прав і свобод, функцій і повноважень.

Окремо визначено такий напрям, як *міжнародна інформаційна діяльність*, що реалізується у двох аспектах:

- забезпечення громадян, державних органів, підприємств, установ і організацій офіційною документованою або публічно оголошуваною інформацією про зовнішньополітичну діяльність України, про події та явища в інших країнах;
- цілеспрямоване поширення за межами України державними органами і об'єднаннями громадян, засобами масової інформації та громадянами всебічної інформації про Україну.

Викремлено чотири основних *види інформаційної діяльності* (ст. 14 Закону України “Про інформацію”):

- *одержання інформації* – набуття, придбання, накопичення відповідно до чинного законодавства України документованої або публічно оголошеної інформації громадянами, юридичними особами або державою;
- *використання інформації* – задоволення інформаційних потреб громадян, юридичних осіб і держави;
- *поширення інформації* – розповсюдження, опрлюднення, реалізація в установленому законом порядку документованої або публічно оголошеної інформації;
- *зберігання інформації* – забезпечення належного стану інформації та її матеріальних носіїв.

Кожен вид інформаційної діяльності вирізняється специфічними правилами та порядком його здійснення, які встановлюються правовими нормами.

2. 6. Інформаційний простір та інформаційний суверенітет.

Основним призначенням права та окремих його норм є регулювання суспільних відносин, яке здійснюється способом цілеспрямованого впливу на свідомість та волю людей. Цей регулятивний вплив характеризується терміном “*дія права*”, що означає перехід соціальних моделей та абстрактних цінностей в реальну практику – в поведінку окремої особи, поведінку соціальних спільнот, спосіб життя суспільства⁷². Дія права та окремих правових норм має певні обмеження, відомі як дія правової норми у просторі, часі та за колом осіб. Загалом основні принципи дії норм інформаційного права аналогічні принципам дії інших правових норм.

Неоднозначним є питання дії норм інформаційного права у просторі. Можна користуватися загальною концепцією, за якою дія норм права обмежена територією держави і пов’язана з такими ознаками державності, як суверенітет та юрисдикція.

Проте деякі ознаки об’єкта інформаційних правовідносин – інформації та загальновизнані принципи регулювання інформаційних відносин змушують нас зробити певні застереження.

⁷² Теория государства и права / Под. ред. В. К. Бабаева. – М. : Юрист, 1999 – С. 443.

Оскільки інформація є нематеріальною субстанцією, вона може бути подана не лише на матеріальних носіях, а й у формі сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб. Такі способи подання інформації дають змогу вільно поширюватися в навколишньому середовищі незважаючи на державні кордони або правові заборони чи приписи. Таким чином, значно зменшується ефективність національних правових норм в регулюванні низки інформаційних відносин: транскордонне теле- і радіомовлення, супутникове теле-радіомовлення, міжнародні телекомунікації, розповсюдження інформації в Інтернет та ін.

Крім того, низка міжнародно-правових актів визначає, що принцип свободи інформації не є обмеженим державними кордонами. Так, Міжнародний пакт про громадянські і політичні права (ч. 2. ст. 19) встановлює “свободу шукати, одержувати і поширювати будь-яку інформацію та ідеї, незалежно від державних кордонів”⁷³. Аналогічне положення, щодо реалізації свободи слова незалежно від кордонів держави міститься і в ст. 10 Конвенції про захист прав і основних свобод людини 1950 р. Подібний підхід реалізується і в нормах національного законодавства. Так відповідно до ч. 2 ст. 50 Закону України “Про інформацію”, що регулює питання міжнародної інформаційної діяльності, громадяни України мають право на вільний і безперешкодний доступ до інформації через зарубіжні джерела, пряме телевізійне мовлення, радіомовлення і пресу.

Таким чином, у законодавстві різних країн створюються певні конструкції, які повинні визначити межі відання держави в інформаційній сфері. Закон України “Про інформацію” (ст. 53) використовує таку дефініцію, як “інформаційний суверенітет”. Визначення цього поняття в цьому Законі не дається, але зазначається, що “основою інформаційного суверенітету України є національні інформаційні ресурси”. До інформаційних ресурсів України, які вона самостійно формує на своїй території та якими вільно розпоряджається, “входить вся належна їй інформація, незалежно від змісту, форм, часу і місця створення”.

Цей Закон (ст. 54) визначає також гарантії інформаційного суверенітету України, який забезпечується:

1) виключним правом власності України на інформаційні ресурси, що формуються коштом державного бюджету;

⁷³ Міжнародний пакт про громадянські і політичні права. Прийнято 16 грудня 1966 р. Генеральною Асамблеєю ООН. Док. ООН А/RES/2200 А (XXI).

- 2) створенням національних систем інформації;
- 3) установленням режиму доступу інших держав до інформаційних ресурсів України;
- 4) використанням інформаційних ресурсів на основі рівноправної співпраці з іншими державами.

Використання в українському законодавстві виразу “інформаційний суверенітет” вже неодноразово викликало сумніви, тим більше, що він не є поширеним в інформаційному законодавстві інших країн і не дістав визнання на міжнародному рівні. Цілком справедливою є думка, що “в часи демократизації, найширшого запровадження сучасних інформаційних технологій вельми проблематично говорити про інформаційний суверенітет на територіальному рівні, тобто в аспекті недоторканості кордонів, недопущення зазіхань на територію тощо”⁷⁴.

На сучасному етапі для характеристики просторових меж державного регулювання інформаційних відносин популярною є дефініція “інформаційний простір”. Зокрема, цей термін дістав широке визнання в нормативно-правових актах та практиці Європейського Союзу. Так, у червні 2005 р. керівними органами ЄС було розпочато реалізацію Стратегії “i2010 – Європейське інформаційне суспільство для зростання та зайнятості”⁷⁵. Першочерговим завданням Стратегії i2010 є створення Єдиного Європейського інформаційного простору, який має стати першою опорою Європейського інформаційного суспільства, що розбудовується.

Єдиний Європейський інформаційний простір, як зазначено в програмних документах, “відкриває відкритий, конкурентний та наповнений контентом (інформаційними ресурсами) внутрішній ринок для електронних засобів зв’язку, мас-медіа та контенту” і “пропонує доступні та безпечні високошвидкісні комунікації, багаті та різноманітні інформаційні ресурси та цифрові послуги”. Крім того, важливим елементом Єдиного європейського інформаційного простору виступає мережева та інформаційна безпека⁷⁶.

Розбудова цього Єдиного інформаційного простору розглядається як відповідь на виклики, поставлені інформаційною революцією, розвитком телекомунікацій та глобалізацією, які впливають на всі ас-

⁷⁴ Баранов А. Информационный суверенитет или информационная безопасность? // Національна безпека і оборона. - № 1, 2001. - с. 71.

⁷⁵ i2010 – A European Information Society for growth and employment, COM(2005) 229.

⁷⁶ COUNCIL RESOLUTION of 22 March 2007 on a Strategy for a Secure Information Society in Europe // Official Journal of the European Union C 68, 24. 3. 2007.

пекти діяльності урядів. Завдання органів ЄС у цьому разі визначається як створення для цього простору сучасної, ринково-орієнтованої правової бази. Така база складається із блоків правових норм, спрямованих на:

- регулювання електронних телекомунікацій;
- розподіл спектра радіочастот;
- створення єдиної аудіовізуальної політики;
- створення нових, багатомовних та інноваційних інформаційних ресурсів;
- створення безпечного інформаційного суспільства.⁷⁷

Наведений приклад, ілюструє основні напрями розвитку інформаційного законодавства на сучасному етапі та спосіб, яким держави й уряди можуть ефективно відповідати на виклики інформатизації та глобалізації.

Отже, можна визначити *єдиний інформаційний простір як сукупність засобів телекомунікації, інформаційних ресурсів та інформаційних послуг, суспільні відносини які регулюються на основі єдиних принципів та правил, що дає змогу забезпечувати захист та реалізацію прав і свобод людини в галузі інформації, функціонування внутрішнього інформаційного ринку та захист інформаційної безпеки.*

Єдиний інформаційний простір виступає як його просторове обмеження дії норм інформаційного права.

Складові – безпосередні об'єкти суспільних інформаційних відносин:

- сама інформація як інформаційний ресурс;
- засоби телекомунікації;
- інформаційні послуги.

Усі складові інформаційного простору пов'язані єдністю тих правил поведінки, тобто правових норм, що регулюють суспільні відносини котрі виникають щодо них.

Основними сферами правового регулювання в межах Єдиного інформаційного простору є такі:

- захист прав і свобод людини в галузі інформації;
- регулювання інформаційного ринку;
- захист інформаційної безпеки.

⁷⁷ Див. : Annual Information Society Report 2007 A European Information Society for Growth and Employment / COM (2007) 146. SEC (2007) 395. – Volumes 1,2,3 – March 2007. – p. 10 – 11.

Завдання щодо розбудови та розвитку єдиного інформаційного простору вирішуються через здійснення процесів *інформатизації* та проведення відповідної *державної інформаційної політики*.

Відповідно до норм ст. 6 Закону України “Про інформацію”, державна інформаційна політика є сукупністю основних напрямів і способів діяльності держави з одержання, використання, поширення та зберігання інформації.

Головними напрямками і способами державної інформаційної політики є:

- забезпечення доступу громадян до інформації;
- створення національних систем і мереж інформації;
- зміцнення матеріально-технічних, фінансових, організаційних, правових і наукових основ інформаційної діяльності;
- забезпечення ефективного використання інформації;
- сприяння постійному оновленню, збагаченню та зберігання національних інформаційних ресурсів;
- створення загальної системи охорони інформації;
- сприяння міжнародній співпраці в галузі інформації і гарантування інформаційного суверенітету України;
- сприяння задоволенню інформаційних потреб українців за кордоном.

Фактично виникнення такого поняття, як “єдиний інформаційний простір” пов’язане із виявленими науковцями ще наприкінці 80-х – початку 90-х років ХХ ст. змінами в житті та взаємодії держави, суспільства й людини, що зумовлені процесами глобалізації та інформатизації. Спричинений ними “зсув” влади, її переорієнтація на нові способи соціального управління, стосуються такого аспекту, як просторове буття держави та відповідно просторова дія санкціонованих державою правових норм. У галузі інформаційних відносин це зумовило зміщення сфери правового регулювання від чіткої прив’язки до території держави до категорії єдиного інформаційного простору. Разом це слід розглядати не як явище що відбулося, а як процес, такий самий, як і формування інформаційного суспільства. І кінцеві результати цього процесу поки що невідомі.

ГЛАВА 3.

ГАРАНТІЇ ПРАВ І СВОБОД ЛЮДИНИ У СФЕРІ ІНФОРМАЦІЇ ЯК БАЗИС ІНФОРМАЦІЙНОГО ПРАВА

*Міжнародно-правові стандарти прав людини
в інформаційній сфері та їх класифікація.
Конституційні засади прав і свобод людини
в інформаційній сфері. Підстави та випадки
обмеження прав людини у сфері інформації.*

3. 1. Міжнародно-правові стандарти прав людини в інформаційній сфері та їх класифікація

Гарантії прав і свобод людини щодо інформаційної сфери належать до найважливіших засад формування правової держави та громадянського суспільства. Ці права перебачені і в дієвому механізмі державного управління в демократичному суспільстві. Це робить забезпечення захисту прав і свобод людини в інформаційній сфері однією з найважливіших цілей інформаційної безпеки, а саму людину – найголовнішим її об'єктом.

Специфіка інформаційної безпеки людини, на відміну від державної безпеки, полягає передусім у чітких і дієвих гарантіях прав і свобод людини в сфері інформації. Слід зазначити, що права на свободу інформації, свободу думки і слова належать до так званих прав “першого покоління” – громадянських і політичних прав, які від початку вважалися і вважаються невід’ємною частиною людської особистості. Права і свободи людини у сфері інформації є важливим чинником умов існування конкретного індивіда і багато в чому визначає політичний устрій держави. Адже права і свободи людини у сфері інформації є ключовими інститутами громадянського суспільства, правової, демократичної держави. Реалізація прав на інформацію, свободу слова є найважливішим механізмом захисту прав людини. В одній із доповідей Уповноваженого Верховної Ради України з прав людини зазначено, що світова практика демократичного державотворення переконує в тому, що право на свободу думки і слова, на вільне вияв-

лення своїх поглядів і переконань є одним з наріжних каменів розбудови демократичної, правової держави і громадянського суспільства. Без свободи слова немає демократії⁷⁸. Важливість права людини на інформацію підкреслюється і в резолюції 59 (1) Генеральної Асамблеї ООН: “свобода інформації є основним правом людини і критерієм усіх інших свобод”.

У другій половині ХХ ст. утвердилися наднаціональні, міжнародні засоби захисту прав людини, які спиралися на розуміння того, що додержання прав людини не може вважатися внутрішньою справою держави. Українське законодавство також визнає пріоритет міжнародно-правових норм над національними, що визначається нормами ст. 9 Конституції України та Законом України “Про міжнародні договори України”. Крім того, згідно з нормами ч. 3 ст. 55 Конституції України, “кожен має право після використання всіх національних засобів правового захисту звертатися за захистом своїх прав і свобод до відповідних міжнародних судових установ чи до відповідних органів міжнародних організацій, членом або учасником яких є Україна”⁷⁹, що створило реальні правові передумови для більш ефективного захисту громадянами своїх прав.

Розвиток міжнародних інструментів захисту прав людини сприяв тому, що “в сучасному міжнародному праві сформувалася галузь, об’єктом якої є міжнародні відносини в області прав людини і основних свобод”⁸⁰. Міжнародно-правові акти, інструменти та інституції, що забезпечують права людини у разі недостатності або недієвості національних інструментів захисту, важливим елементом інформаційної безпеки.

Головним міжнародно-правовим стандартом у галузі прав людини є комплексний акт, розроблений в рамках ООН і відомий як *Хартія про права людини*. Ця Хартія складається із Загальної декларації прав людини, Міжнародного пакту про економічні, соціальні і культурні права та Міжнародного пакту про громадянські та політичні права. Ці акти стали головним стандартом, базою, на основі яких було розроблено низку інших міжнародних та національних правових актів в галузі прав людини, в т. ч. відповідних розділів конституцій багатьох

⁷⁸ Карпачова Н. І. Стан дотримання та захисту прав і свобод в Україні: Перша щорічна доповідь Уповноваженого Верховної Ради України з прав людини. – К., 2000. – С. 202.

⁷⁹ Конституція України. Прийнята Верховною Радою України 28 червня 1996 р. // Відомості Верховної Ради. – 1996. – N 30. – Ст. 141.

⁸⁰ Тимченко М. Д. Международное право. – Харьков: Консум, 1999. – С. 107.

держав світу, зокрема Розділ II “Права, свободи та обов’язки людини і громадянина” Конституції України 1996 р.

Першим фундаментальним, міжнародно-правовим актом у рамках Хартії про права людини є *Загальна декларація прав людини*, прийнята Генеральною Асамблеєю ООН 10 грудня 1948 р. Вона містить комплекс юридичних гарантій, що визначають зміст і сутність інформаційної безпеки особи.

Так, за нормами ст. 19 Загальної декларації прав людини встановлено “кожна людина має право на свободу переконань і на вільне їх виявлення; це право включає свободу безперешкодно дотримуватися своїх переконань та свободу шукати, одержувати і поширювати інформацію та ідеї будь-якими засобами і незалежно від державних кордонів”⁸¹.

Подібне розуміння права на свободу інформації поширилося в багатьох міжнародних та національних правових актах і перетворилося на певний еталон демократичного суспільства, лакмусовим папірцем ситуації з дотриманням прав людини у будь-якій державі. Це право є “активним” за змістом, оскільки виражає певну міру поведінки. Для його реалізації людина має вдатися до активних дій.

Дещо іншим за змістом є право, передбачене ст. 12 Декларації. Воно полягає в тому, що “ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя, безпідставного посягання на недоторканність його житла, таємницю його кореспонденції або на його честь і репутацію”. Передбачається також, що “кожна людина має право на захист закону від такого втручання або таких посягань”.

Останні норми, в принципі, не вимагають від суб’єкта відповідних дій щодо їх реалізації, а навпаки, обмежують дії інших суб’єктів інформаційних відносин, захищаючи відповідні інформаційні відносини, що склалися. Це типовий вид норми-заборони, згідно з якою охоронні правовідносини (захист закону від неправомірного втручання) виникають у разі їх порушення.

Отже, можна стверджувати, що правовий статус людини як суб’єкта інформаційних відносин ґрунтується на двох основних її правах:

1) право вільно, безперешкодно, на власний розсуд бути суб’єктом інформаційних процесів, шукати, одержувати і поширювати інфор-

⁸¹ Загальна декларація прав людини. Прийнята Генеральною Асамблеєю ООН 10 грудня 1948 р. /Док. ООН/PES/217 А.

мацію, причому це право не пов'язане з територіальною юрисдикцією держави і не обмежується територіально державними кордонами;

2) це право на захист від неправомірного інформаційного втручання *privacy*, тобто право на конфіденційність інформації про особисте життя та на захист від розповсюдження вигаданої й перекрученої інформації, що завдає шкоди честі й репутації особи.

Подібна конструкція прав людини в галузі інформації, як уже зазначалося, була сприйнята як стандарт і в міжнародному, і національному праві більшістю держав світу, в т. ч. й Україною, та відтворена у багатьох нормативно-правових актах.

Зокрема, аналогічні за змістом норми є в *Міжнародному пакті про громадянські і політичні права*, прийнятому Генеральною Асамблеєю ООН 16 грудня 1966 р.

Аналогічна за змістом, але відмінна за формою викладення в правових нормах конструкція відтворена і в *Конвенції про захист прав і основних свобод людини* 1950 р.⁸² Ця Конвенція є особливо актуальною для України з огляду на ратифікований нашою державою Протокол 11, який передбачає можливість захисту прав і свобод, встановлених цією Конвенцією, у Європейському суді з прав людини. При цьому слід звернути увагу не тільки на правові норми, викладені у відповідних статтях Конвенції, а й на практику Суду з їх застосування і тлумачення, оскільки така практика має прецедентний характер і використовується під час ухвалення наступних рішень Суду з аналогічних питань.

Ст. 10 Конвенції *свободу вираження поглядів*: “Кожен має право на свободу вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів”.

Практика Суду значною мірою конкретизує цю норму, серед яких, зокрема, виражає такі позиції:

- термін “вираження поглядів” означає подання інформації в будь-якій формі (документи, промови, зображення, дії, що виражають позицію чи подають інформацію, тощо), а також за допомогою будь-яких засобів (наприклад, друковані й електронні ЗМІ, кінофільми, вистави тощо). Таким чином, захист поширюється не лише на саме вираження поглядів, а й на за-

⁸² Конвенція про захист прав і основних свобод людини 1950 року, Перший протокол та протоколи № 1, 4, 6, 7, 9, 10 та 11 до Конвенції (Рим, 4. 11. 1950) / Голос України. – 2001 р. – № 3 (2503). – С. 6 – 8.

соби такого вираження. Захищається не лише вираження політичних поглядів, а й діяльність у мистецькій сфері та інформація комерційного характеру;

- існує відмінність між поняттями “інформація” та “ідея”. Відтак свобода висловлювань не обмежується лише фактичними даними, які можна підтвердити, а передбачає також погляди, критику й припущення. Отже вимагати доведення правдивості або спростування можна лише стосовно фактів. Особа, котра висловила свої погляди, а не факти, не зобов’язана їх доводити.⁸³

Нормами ст. 8 Конвенції визначено *право на повагу до приватного і сімейного життя*: з “Кожен має право на повагу до його приватного і сімейного життя, до житла і до таємниці кореспонденції”.

У контексті цієї норми можна зазначити:

- дотримання права на приватне життя передбачає обов’язок держави контролювати діяльність як органів публічної влади та їх посадових осіб, так і фізичних та юридичних осіб;
- навіть якщо факт збирання інформації про особисте життя є виправданим з огляду на закон, її подальше зберігання або використання може бути правопорушенням;
- при забезпеченні таємниці кореспонденції держава не зобов’язана забезпечувати зразкове функціонування поштових послуг⁸⁴.

Наведені вище міжнародно-правові акти мають універсальний характер, визначаючи основні права і свободи людини.

Разом із тим питання реалізації та захисту окремих видів прав людини у сфері інформації дістали відображення в інших актах міжнародного права, серед яких:

Конвенція про доступ до інформації, участь громадськості в процесі прийняття рішень та доступ до правосуддя з питань, що стосуються довкілля, підписана 28 червня 1998 р. в м. Орхус, Данія⁸⁵. Визначає основні принципи надання громадськості екологічної інформації органами державної влади та місцевого самоврядування. Укра-

⁸³ Див.: Огляд практики Європейського суду з прав людини. Норми і стандарти Конвенції про захист прав і основних свобод людини. – К. : Мін-во юстиції України, 2002. – С. 37.

⁸⁴ Див.: Там само. – С. 28 – 31.

⁸⁵ Конвенція про доступ до інформації, участь громадськості в процесі прийняття рішень та доступ до правосуддя з питань, що стосуються довкілля Від 28 червня 1998 р. (Ратифіковано Законом України № 832-ХІV від 6 липня 1999 р.) // Відомості Верховної Ради України. – 1999. – № 34. – Ст. 296.

їна ратифікувала цю Конвенцію 6 липня 1999 р., її положення були імplementовані в національне законодавство України.

Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру, підписана в Страсбурзі 28 січня 1981 р.⁸⁶. Ст. 1 цієї Конвенції роголошує забезпечення на території кожної держави-учасниці для кожної особи незалежно від її національності або помешкання поважання її прав і основних свобод, зокрема її права на недоторканність особистого життя, стосовно автоматизованої обробки даних особистого характеру.

Конвенцією визначено (ст. 5) основні вимоги до інформації особистого характеру, що піддається автоматизованій обробці. Ці дані про особу мають бути:

- отримані та оброблені сумлінно й законно;
- зберігатися для визначених і законних цілей і не використовуватися у спосіб, несумісний із цими цілями;
- адекватними, відповідними й ненадмірними з огляду на цілі, заради яких вони зберігаються;
- точними і в разі потреби мають поновлюватися;
- зберігатися у форматі, який дає змогу ідентифікувати суб'єктів даних не довше, ніж це потрібно для цілей, заради яких такі дані зберігаються.

З метою гарантування дотримання прав осіб до таких даних мають застосовуватися засоби захисту щодо запобігання випадковому знищенню або несанкціонованому доступу, змінам або поширенню (ст. 7).

Передбачені також додаткові права особи – суб'єкта даних (ст. 8), зокрема можливість:

- встановлювати існування файлу даних особистого характеру;
- отримувати такі дані в доступній для розуміння формі;
- вимагати у відповідних випадках виправлення або знищення таких даних;
- використовувати засоби правового захисту.

Слід зазначити, що для України є дуже актуальним є приєднання до цієї Конвенції з огляду на наявність систематичних порушень прав громадян щодо розголошення даних особистого характеру, які збирають органи публічної влади згідно із їх компетенцією. Крім того, питання прав людини у сфері інформації та стану їх захисту розгля-

⁸⁶ Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру. Страсбург, 28 січня 1981 р. / Збірка договорів Ради Європи. – К.: Парламентське вид-во, 2000.

даються в деяких документах міжнародних міжурядових організацій, насамперед ООН, Ради Європи, ОБСЄ та ін. Деякі із цих документів стосуються й України, наприклад рекомендації Ради Європи.

3. 2. Конституційні засади прав і свобод людини в інформаційній сфері

Конституція України надає людині як об'єкту безпеки особливого статусу, встановлюючи формулу відносин між особою і державою за формою держава для людини, а не навпаки, як це незрідка було протягом історії людства. Згідно зі ст. 3. Конституції України, людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю⁸⁷. Підкреслюється, що права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави, а їх утвердження і забезпечення є головним обов'язком держави.

Конституція України, визначаючи комплекс прав людини в галузі інформації, базується на міжнародно-правових стандартах у цій галузі і відтворює як концептуально, так і змістовно переважно відповідні їх положення. Ключовими для визначення прав і свобод людини в галузі інформації є норми статей 34 і 32 Конституції.

Так, ст. 34 Конституції визначає *право на свободу слова та право на інформацію*, згідно з яким:

- кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань;
- кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір”.

Ч. 3 ст. 34 Конституції містить вичерпний перелік випадків обмеження цього права.

Ст. 40 Конституції визначає *право на звернення* як механізм, за допомогою якого особа може реалізовувати свої права законні інтереси у відносинах з органами публічної влади, зокрема в тому, що стосується доступу та отримання інформації від цих органів. За цією статтею, усі мають право направляти індивідуальні чи колективні письмові звернення або особисто звертатися до органів державної влади,

⁸⁷ Конституція України. Прийнята Верховною Радою України 28 червня 1996 р. // Відомості Верховної Ради. – 1996. – № 30. – Ст. 141.

органів місцевого самоврядування та посадових і службових осіб цих органів, котрі зобов'язані розглянути звернення і дати обґрунтовану відповідь у встановлений законом строк.

Установлене ст. 34 Конституції право є “активним” за своїм змістом, оскільки визначає певну міру поведінки. Для його реалізації людина має вдатися до активних дій. Це право людини може розумітися як можливість здійснювати будь-яким способом та у будь-якій формі бути учасником інформаційних відносин, крім випадків, коли існують прямі заборони законом.

Інша група прав людини в галузі інформації, встановлена Конституцією, спрямована на обмеження інформаційного втручання у приватні справи особи з боку держави і третіх осіб. Ці норми мають передусім, захисний характер щодо конкретних правових відносин в інформаційній сфері.

Гарантії *права людини на невтручання в особисте життя*, ґрунтуються насамперед на ст. 32 Конституції, яка, зокрема, визначає, що: “Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України.

Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини”. Нормами цієї статті визначаються і основні механізми забезпечення зазначеного права. Першим із них (ч. 3 ст. 32 Конституції) є право громадянина ознайомлюватися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею. Це право дає змогу встановити сам факт збирання інформації про особу органами публічної влади та їх посадовими особами, визначити їх зміст і на підставі цього установити ступінь правомірності таких дій.

Інший механізм (ч. 4 ст. 32 Конституції) полягає в гарантії судового захисту прав:

- спростовувати недостовірну інформацію про себе і членів своєї сім'ї;
- вимагати вилучення будь-якої інформації;
- відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації.

Похідним від права на невтручання в особисте життя є *право на таємницю кореспонденції*, оскільки фактично цим правом встановлюється додаткова гарантія невтручання в особисте життя людини. Зокрема, в рамках Конвенції про захист прав і основоположних свобод людини (ст. 8) ці права розглядаються в комплексі. В Конституції України це право визначено окремою ст. 31, за якою кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Основним механізмом забезпечення цього права є визначене в ст. 8 правило, згідно з яким винятки із права на таємницю кореспонденції можуть бути встановлені лише судом з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо.

Зазначені вище основні права людини в інформаційній сфері підкріплюються і розширюються низкою інших конституційних норм. Зокрема, ст. 15 Конституції України, встановлює політичну й ідеологічну багатоманітність суспільного життя і забороняє цензуру; ст. 21 – закріплює невідчужуваність та непорушність прав і свобод людини; ст. 28 – закріплює право людини на повагу до її гідності, забороняє піддавати людину катуванню, жорстокому, нелюдському або такому, що принижує її гідність, поводженню чи покаранню; піддавати людину без її вільної згоди медичним, науковим чи іншим досліддам. Ст. 41 Конституції визначає право кожного володіти, користуватися й розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності та встановлює непорушність права приватної власності.

Проте певну “бомбу сповільненої дії”, закладено в розділі II Конституції. Це зумовлено тим, що вітчизняна правова наука практично не сприймає існуючу в західному конституційному праві класифікацію термінів для визначення прав людини. Так, в англійській термінології використовуються поняття: *rights* – для визначення невід’ємних прав людини (на життя, свободу тощо); *freedoms* або *liberties* – для визначення громадських і політичних прав і свобод і термін *entitlements*, який охоплює надані державою економічні і соціальні права. В українському законодавстві натомість застосовується єдиний термін “права людини”. Так, разом з уже названими інформаційними правами і свободами в Конституції України виначено низку прав, які є інформаційними за своїм об’єктом, але економічними або соціальними за своїм змістом.

Це передусім норми ст. 54, які встановлюють: «Громадянам гарантується свобода літературної, художньої, наукової і технічної творчості, захист інтелектуальної власності, їхніх авторських прав, моральних і матеріальних інтересів, що виникають у зв'язку з різними видами інтелектуальної діяльності.

Кожний громадянин має право на результати своєї інтелектуальної, творчої діяльності; ніхто не може використовувати або поширювати їх без його згоди, за винятками, встановленими законом.

Держава сприяє розвитку науки, встановленню наукових зв'язків України зі світовим співтовариством.

Культурна спадщина охороняється законом.

Держава забезпечує збереження історичних пам'яток та інших об'єктів, що становлять культурну цінність, вживає заходів для повернення в Україну культурних цінностей народу, які знаходяться за її межами»⁸⁸

Але чи можна, наприклад, розвиток наукових зв'язків або правове регулювання використання об'єктів інтелектуальної власності ставити в один ряд із невід'ємними інформаційними правами людини на таємницю приватного життя, на свободу слова, на захист честі й гідності? До того ж, простий аналіз норм Конституції вказує на похідний характер інформаційних прав, зазначених у ст. 54. Так право на свободу літературної, художньої, наукової і технічної творчості є складовою права на свободу слова, встановленого ст. 34 Конституції, права щодо захисту інтелектуальної власності є похідними від загального права власності (в т. ч. й інтелектуальної), визначеного у ст. 41 Конституції тощо.

У чому ж полягає небезпека, зумовлена відсутністю чіткого поділу в Конституції громадянських прав і свобод та економічних і соціальних прав людини? Чинників безпеки ми можемо виділити щонайменше два. Один – у сфері правової свідомості, другий – у сфері практики правозастосування, обидва чинники є взаємопов'язані.

Зміст першого чинника безпеки полягає в підміні політичних проблем соціально-економічними і, відповідно, зменшенні уваги до захисту невід'ємних прав і свобод. Результати багатьох соціологічних досліджень свідчать про те, що увага населення до питань економічних прав – рівня життя, зайнятості, економічного стану взагалі, все

⁸⁸ Конституція України. Прийнята Верховною Радою України 28 червня 1996 р. // Відомості Верховної Ради. – 1996. – № 30. – Ст. 141.

ще значно переважає увагу до політичних, зокрема до свободи слова. Таким чином, фактично вимикається такий важливий інструмент демократії, як громадський контроль за владою, котрий більшість фахівців розглядає як єдино можливий механізм подолання більшості проблем у взаємовідносинах між владою і суспільством. Таке розходження теорії з практикою полягає “у декларативності багатьох із тих прав, реалізація яких робить суспільство стабільним і в економічному, і в політичному плані”⁸⁹.

У чому ж полягає ця декларативність, насамперед щодо прав і свобод людини у сфері інформації, що має такий руйнівний вплив на демократичні процеси в Українській державі та суспільстві?

Сам термін забезпечення конституційних прав і свобод людини і громадянина – “це система їх гарантування з боку державних інститутів, яка функціонує у правовому режимі і до якої належать такі елементи, як компетенція, охорона, захист, а також створення необхідних умов для реальної реалізації людиною своїх прав і свобод”⁹⁰. У цьому аспекті засоби забезпечення слід поділити на правові – безпосередньо охорона і захист за допомогою юридичних механізмів та організаційні – створення необхідних умов у процесі діяльності органів публічної влади.

Згідно з ч. 3 ст. 8 Конституції України, її норми є нормами прямої дії, і кожному гарантується звернення до суду для захисту конституційних прав і свобод людини і громадянина безпосередньо на підставі Конституції України.

Виконання інформаційних прав людини, які належать до громадянських та політичних прав і свобод (свобода слова, право на одержання інформації, право на невтручання в особисте життя, право на таємницю листування, заборона цензури) може бути повною мірою забезпечене судовими органами, як це і передбачено ст. 55 Конституції України. Для реалізації громадянських та політичних прав достатньо застосування виключно правових механізмів: правильне застосування судами конституційних норм та відповідного галузевого законодавства, прийняття судового рішення та його виконання.

⁸⁹ *Кормич Л. І.* Права людини: від декларацій до гарантій // Актуальні проблеми політики. 36. наук. праць. – Одеса: Юрид. літ-ра, 2001. – Вип. 12. – С. 8 – 9.

⁹⁰ *Степаненко К. В.* Еволюція терміна “забезпечення” щодо прав і свобод людини // Держава і право: 36. наук. праць. Юридичні і політичні науки. – Вип. 15. – К.: Ін-т держави і права ім. В. М. Корецького НАН України. – С. 178.

Реалізація багатьох соціальних і економічних прав залежить не тільки від нормативно-правових приписів, а й від забезпечення відповідних умов. Останнє є компетенцією не судової, а насамперед виконавчої гілки влади та місцевого самоврядування. Наприклад, рішення суду замало для забезпечення розвитку науки або збереження культурної спадщини, адже такі завдання вимагають матеріального забезпечення. Типовим прикладом ситуації із соціальними та економічними правами є низка рішень Конституційного Суду щодо неконституційності окремих положень Законів України “Про державний бюджет”, якими припинялася дія норм інших законодавчих актів щодо соціальних гарантій. Як зазначалося в Рішенні Конституційного Суду у справі про соціальний захист громадян (п. 3. 2.), “Конституційний Суд України неодноразово розглядав за зверненнями суб’єктів права на конституційне подання справи і приймав рішення, у яких визнавав окремі положення законів про Державний бюджет України щодо зупинення або обмеження пільг, компенсацій і гарантій такими, що не відповідають Конституції України... Проте, незважаючи на зазначені рішення Конституційного Суду України, ревізія законами про Державний бюджет України пільг, компенсацій і гарантій, яку започатковано у 1995 році, набула системного характеру”⁹¹. Проблема з виконанням подібних рішень полягає в тому, що Суд, визнавши неконституційним певну норму закону, що обмежує соціальне або економічне право, не може створити нову норму, яка б забезпечила фінансування реалізації такого права.

Отже, ситуація коли виконання соціальних та економічних прав не завжди може бути забезпеченим виключно судовою гілкою влади, як це передбачено нормами ст. 55 Конституції України, створює прецедент, коли закріплені в Конституції права людини порушуються, а механізм їх забезпечення не діє. В свою чергу, безкарне, можливо, незначне на перший погляд порушення бодай одного конституційного права може потягти за собою більш значні й фатальні порушення інших прав. Адже, як зазначалося у одному з рішень Європейського Суду з прав людини, “Різниця полягає лише в мірі утиску, а історія

⁹¹ Рішення Конституційного Суду України у справі за конституційним поданням 46 народних депутатів України щодо відповідності Конституції України (конституційності) положень статей 29, 36, частини другої статті 56, частини другої статті 62, частини першої статті 66, пунктів 7, 9, 12, 13, 14, 23, 29, 30, 39, 41, 43, 44, 45, 46 статті 71, статей 98, 101, 103, 111 Закону України “Про Державний бюджет України на 2007 рік” (справа про соціальні гарантії громадян) від 9 липня 2007 р. № 6-рп/2007.

вчить нас, що влада, яка свавільно порушує одне право, скоро перестане поважати й інші”⁹².

На небезпеці подібної ситуації наголошувалося і у висновку Венеціанської комісії від 11 березня 1996 р. щодо проекту, на основі якого було прийнято Конституцію України. Зокрема, в цьому висновку було висловлено зауваження і вказано на певні недоліки у розділі “Права і свободи людини і громадянина”, серед яких були такі: вичерпність наведених у цій главі прав, що включає права соціального, економічного та екологічного характеру, створює проблеми щодо забезпечення їх гарантіями судового захисту; можливі обмеження та стримування основних прав часто заходять надто далеко⁹³.

Незважаючи на те, що судовий захист визначено Конституцією як самодостатній механізм забезпечення прав і свобод людини, він є лише одним із елементів системи забезпечення цих прав.

Так, розглядаючи питання реалізації конституційних гарантій, не можна не відзначити важливість органів виконавчої влади і місцевого самоврядування. Повсякденна діяльність цих органів має створювати відповідні умови для реалізації громадянами своїх прав і законних інтересів. Адже “саме через канали виконавчої влади відбувається реалізація прав і свобод людини і громадянина”⁹⁴. Концепція адміністративної реформи, реформи адміністративного права та інші документи спрямовані на зміну самих поглядів на сутність державної влади та закріплення підходу, за якого “державна влада – це реалізація не тільки правомочностей, що зобов’язують громадянина, а й виконання певних обов’язків держави перед громадянином, за які вона цілком відповідальна перед ним. І таких обов’язків з її боку з’являтиметься дедалі більше в міру демократизації Української держави”⁹⁵. Подібне твердження аж ніяк не принижує значення судового захисту, адже, згідно з ч. 2 ст. 124 Конституції України, юрисдикція судів поширюється на всі правовідносини, що виникають у державі. Але судовий захист застосовується у випадках, коли вже відбулося порушення права, а завдання виконавчої влади створити умови, за яких подібні порушення не відбуватимуться. Адже саме до компетенції органів виконавчої влади віднесено “процес створення умов, необхідних для здійснення використання прав людини, який включає у себе такі елемен-

⁹² Dash vs. Van Kleek., 7 Johns. (N. Y.) 477, 506 (1811).

⁹³ Конституція незалежної України. – Кн. 2. – Ч. 1. – С. 247.

⁹⁴ Заєць А. П. Правова держава в контексті новітнього українського досвіду. – К., 1999. – С. 214.

⁹⁵ Адміністративне право України. Академічний курс. / За ред. В. Б. Авер’янова. – К., 2004 – С. 79.

ти державної діяльності, як сприяння реалізації прав людини, охорона прав людини та захист прав і свобод людини”⁹⁶. Важлива роль адміністративно-правових відносин в гарантуванні права людини на інформацію визначається і Законом України “Про інформацію”, в якому гарантування розглядається саме як створення необхідних умов. Цей Закон (ст. 10) гарантіями права на інформацію називає:

- обов’язок органів державної влади, а також органів місцевого і регіонального самоврядування інформувати про свою діяльність та прийняті рішення; створення у державних органах спеціальних інформаційних служб або систем, що забезпечували б у встановленому порядку доступ до інформації;
- вільний доступ суб’єктів інформаційних відносин до статистичних даних, архівних, бібліотечних і музейних фондів, обмеження якого зумовлюються лише специфікою цінностей та особливими умовами їх збереження, що визначаються законодавством;
- створення механізму здійснення права на інформацію;
- здійснення державного контролю за дотриманням законодавства про інформацію;
- встановлення відповідальності за порушення законодавства про інформацію.

Не менш важливим механізмом є контроль з боку інститутів громадянського суспільства. Причому на прикладі права на свободу слова реалізується цікава взаємозалежність. З одного боку, дотримання цього права неможливе без ефективного громадського контролю, з другого – за відсутності цього права сам громадський контроль буде неефективним. Історія розвитку інституту прав людини свідчить, що, на жаль, найбільших утисків, порушень та обмежень інформаційні права і свободи людини зазнавали з боку держави та її органів, оскільки вступали в конфронтацію з інтересами останніх. Як зазначає відомий американський правник Бернард Сіган, який брав участь у розробленні конституцій деяких східноєвропейських країн: “Конституція повинна турбуватися про свободу в заперечувальному розумінні – захисту особистості від сили влади”⁹⁷. Таку постановку питання прийнято пояснювати схильністю державної влади до самоконцен-

⁹⁶ Рабінович П. М., Панкевич І. М. Здійснення прав людини: проблеми обмежування (загальнотеоретичні аспекти). – Л., 2001. – С. 20.

⁹⁷ Сіган Бернард Г. Створення конституції для народу чи республіки, що здобули свободу. – К.: Ін-т демократії ім. П. Орлика, 1993 – С. 31.

трації та самозростання. В розвиненому демократичному суспільстві подібні небезпечні тенденції повинні компенсуватися системою розподілу влад з її стримуваннями і противагами, а також обмежуватися контролем з боку інститутів громадянського суспільства. Важливість ролі громадськості в забезпеченні конституційних прав і свобод та розбудові державної влади на демократичних засадах підкреслював один із “батьків-засновників” американської нації Бенджамін Франклін ще в 1787 р. , коли Конституційні Збори північноамериканських колоній завершили свою роботу. Тоді на запитання “Так що в нас тепер – республіка чи монархія?”, він відповів: “Республіка, якщо ви її збережете”⁹⁸.

Конституційні засади прав і свобод людини дістають відображення у низці нормативно-правових актів. Деякі з них безпосередньо спрямовані на забезпечення прав і свобод людини в галузі інформації, інші регулюють окремі аспекти цих прав або реалізацію їх у рамках певних видів діяльності.

3. 3. Підстави і випадки обмеження прав людини у сфері інформації

Для забезпечення прав і свобод людини у сфері інформації особливо важливим є визначення міри необхідного втручання держави в інформаційні відносини. Оскільки інформація в суспільстві нерозривно пов’язана з процесами комунікації, то реалізація інформаційних прав одним суб’єктом у будь-якому разі впливає на відповідні права інших суб’єктів.

У Загальній декларації прав людини не визначено конкретних обмежень використання та реалізації людиною свого права на інформацію. Існує лише загальна норма ст. 29 Декларації, яка передбачає, що при здійсненні своїх прав і свобод кожна людина може зазнавати тільки обмежень, установлених законом виключно з метою забезпечення належного визнання і поваги прав і свобод інших та забезпечення справедливих вимог моралі, громадського порядку і загального добробуту в демократичному суспільстві (ч. 2 ст. 29), а також зазначено, що здійснення відповідних прав і свобод в жодному разі не повинне суперечити цілям і принципам Організації Об’єднаних Націй (ч.

⁹⁸ Ferrand M. The records of the Federal Convention of 1787. – New Hayden & London: Yale Univ. Press, 1966. – P. 85.

3 ст. 29). Таким чином, визначено три основні ознаки, які в комплексі можуть бути підставою для обмеження прав і свобод людини: забезпечення прав і свобод третіх осіб або моралі, громадського порядку і загального добробуту, причому, що важливо, лише в тому розумінні, яке існує в рамках демократичного суспільства; забезпечення дотримання цілей і принципів ООН та наявність прямих правових приписів, що регламентують застосування подібних обмежень.

Більш детально баланс між мірою поведінки людини при здійсненні своїх інформаційних прав та мірою втручання держави в цю сферу прописано в нормах Міжнародного пакту про громадянські і політичні права. У п. 2. ст. 19 цього Пакту більш детально прописане право на свободу інформації, яке визначається як право на вільне вираження світогляду і включає: свободу шукати, одержувати і поширювати будь-яку інформацію та ідеї, незалежно від державних кордонів, усно, письмово чи за допомогою друку або художніх форм вираження чи іншими способами на свій вибір. Новелою в цьому аспекті було включення “художніх форм вираження” як засобу розповсюдження інформації. Тобто свобода художньої творчості, мистецтва розглядається саме в контексті свободи інформації. У Пакті, також визначено специфічні принципи регулювання інформаційних відносин з боку держави. Таким чином визнано специфіку інформаційної сфери як складного і важливого напрямку людської діяльності. Зокрема, за п. 3. ст. 19 Пакту користування правом на свободу інформації накладає особливі обов’язки і особливу відповідальність і, отже, це право може бути пов’язане з певними обмеженнями. Викладено конкретні вимоги до встановлення подібних обмежень свободи інформації; ці обмеження “мають встановлюватися законом і бути необхідними: а) для поважання прав і репутації інших осіб; б) для охорони державної безпеки, громадського порядку, здоров’я чи моральності населення”⁹⁹.

Поняття “прав і репутації інших осіб” більшою мірою розкривається у ст. 17 Пакту. До комплексу цих прав включені обмеження дій третіх осіб і держави щодо свавільного чи незаконного втручання в особисте і сімейне життя, свавільних чи незаконних посягань на недоторканність життя особи або таємницю її кореспонденції чи незаконних посягань на її честь і репутацію. Передбачається, що національне законодавство має передбачати механізми захисту від поді-

⁹⁹ Міжнародний пакт про громадянські і політичні права. Прийнято 16 грудня 1966 року Генеральною Асамблеєю ООН. Док. ООН A/RES/2200 A (XXI)

бних посягань і кожна людина повинна мати право скористатися таким захистом.

Повертаючись до питання балансу між свободою інформації та її обмеженням в інтересах захисту прав третіх осіб та безпеки держави, зазначимо, що найбільш детально механізми досягнення цього балансу розроблено в рамках Конвенції про захист прав і основних свобод людини 1950 р. та в практиці діяльності Європейського суду з прав людини. Особливо корисна в цьому аспекті судова практика Європейського суду з прав людини, оскільки застосування норм Конвенції як норм прямої дії дало змогу створити певні принципи і прецеденти, що визначають міру допустимого втручання держави в інформаційну сферу.

У нормах цієї Конвенції¹⁰⁰ разом із відповідними інформаційними правами і свободами прописано низку випадків і умов обмеження цих прав. Так, ст. 6 установлюючи право особи на справедливий і відкритий розгляд її справи упродовж розумного строку незалежним і безстороннім судом, створеним відповідно до закону, передбачає: “Судова постанова оголошується прилюдно, але преса і відвідувачі можуть не допускатися до залу засідань протягом усього судового розгляду або якоїсь його частини з метою збереження моральних засад, громадського порядку або національної безпеки в демократичному суспільстві, коли того вимагають інтереси малолітніх чи захисту конфіденційності особистого життя сторін або у разі неминучої потреби, коли, на думку суду, в особливих випадках привселюдність розгляду може зашкодити інтересам правосуддя”.

Ст. 8 Конвенції визначає, що органи державної влади не можуть втручатися у здійснення права на повагу до приватного і сімейного життя “інакше ніж згідно із законом і коли це необхідно в демократичному суспільстві в інтересах національної і громадської безпеки або економічного добробуту країни, з метою запобігання заворушенням чи злочинам, для захисту здоров’я чи моралі або з метою захисту прав і свобод інших осіб”.

Ст. 10 Конвенції встановлює право людини на свободу виявлення поглядів, яке включає свободу дотримуватися своїх поглядів, одержувати і поширювати інформацію та ідеї без втручання держави і незалежно від кордонів. Разом з тим ця стаття містить дві групи норм, що встановлюють обмеження цього права. Перше обмеження встановлю-

¹⁰⁰ Конвенція про захист прав і основних свобод людини 1950 року, Перший протокол та протоколи № 1, 4, 6, 7, 9, 10 та 11 до Конвенції (Рим, 4. XI. 1950) / “European Treaty Series” – № 5.

ється нормою ч. 1 ст. 10, яка визначає: “Ця стаття не перешкоджає державам вимагати ліцензування радіомовлення, телебачення або кінопідприємств”. Інше обмеження, закріплене нормами ч. 2 ст. 10 Конвенції, визначає: “Здійснення цих (інформаційних – *Б. К.*) свобод, оскільки воно пов’язане з правами та обов’язками, може бути предметом таких формальностей, умов, обмежень або покарання, які встановлені законом і є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням або злочинам, для захисту здоров’я і моралі, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя”.

Таким чином, на основі аналізу наведених правових норм ми можемо визначити конкретні допустимі випадки та умови обмеження прав і свобод особи у сфері інформації. В рамках цього аналізу відразу слід підкреслити, що перелік можливих причин обмеження інформаційних прав і свобод характеризується часткою “лише”, тобто обмеження допускається лише з причин, прямо вказаних у нормах Конвенції, а можливість розширювального тлумачення цього переліку виключається. Крім того, в Конвенції підкреслюється, що обмеження мають стосуватися не самих по собі прав і свобод, а конкретних випадків їх реалізації, щодо яких можуть вводитися додаткові формальності та застереження.

Передбачені Конвенцією випадки і причини обмеження реалізації інформаційних прав людини умовно можна поділити на кілька груп. До першої групи можна віднести дії, необхідні для захисту безпеки держави, зокрема, охорону і захист:

- громадського порядку;
- громадської безпеки;
- національної безпеки;
- територіальної цілісності.

До другої групи ми можна включити розв’язання таких загально-суспільних завдань, як захист:

- здоров’я;
- моральних засад.

Третю групу становлять відповідні заходи захисту прав та інтересів третіх фізичних осіб. Вони включають необхідність забезпечення та захисту:

- прав і свобод інших людей;
- конфіденційності особистого життя;
- репутації інших людей;
- інтересів малолітніх.

У четверту групу можна поєднати завдання, що вирішуються в рамках правоохоронної діяльності держави. Такі обмеження інформаційних прав можливі для:

- запобігання заворушенням або злочинам;
- забезпечення інтересів правосуддя;
- підтримання авторитету і неупередженості правосуддя;
- запобігання розголошенню інформації, одержаної конфіденційно.

І останню, п'яту, групу становлять права держави та її компетентних органів вводити певні процедури щодо ліцензування мас-медіа:

- радіомовлення;
- телебачення;
- кінопідприємств.

Разом із наведеним переліком випадків введення різних формальностей, умов, обмежень або покарань, які можуть застосовуватися до реалізації відповідних прав у сфері інформації, визначаються також умови застосування цих заходів.

Першою і головною умовою встановлення обмежень на реалізацію особою її інформаційних прав визначається те, що *подібні заходи повинні розглядатися як прийнятні в демократичному суспільстві*. Тобто вони мають реалізовуватися в демократичній системі за наявності необхідних механізмів забезпечення прав і свобод людини, громадського контролю, відповідати принципам демократичного суспільства та не суперечити цілям, викладеним у Статуті ООН та інших міжнародно-правових актах.

Не менш важливою є умова, що *обмеження та механізми їх застосування мають бути встановлені законом*. Тобто органи державної влади, що застосовують подібні заходи, мають діяти виключно на основі і в рамках існуючих національних нормативно-правових актів. Застосування таких обмежень за власним розсудом тих чи інших посадових осіб не допускається.

Наступна умова полягає у тому, що *обмеження можна застосовувати лише в особливих випадках*. Це означає, що обмеження свободи інформації та інших пов'язаних із цим прав не повинні мати масо-

вого, загального характеру, а застосовувати їх можна лише у виняткових випадках щодо конкретних ситуацій або конкретних суб'єктів інформаційних відносин за наявності індивідуального підходу до кожного випадку.

Нарешті, подібні обмеження, умови, формальності та покарання можна застосовувати лише в разі неминучої потреби. Це означає, що ці заходи мають бути адекватними існуючим загрозам, суспільна шкода від застосованих обмежень не повинна перевищувати можливої шкоди від наявних загроз. Крім того, державні органи мають застосовувати подібні заходи, лише якщо вони справді необхідні в певній ситуації і ніякими іншими засобами поставлені завдання вирішити неможливо.

Проте більшість норм Конвенції має узагальнений оцінювальний характер, тому виняткового значення набуває практика Європейського суду щодо їх тлумачення. Це передусім стосується випадків і умов застосування обмежень щодо реалізації інформаційних прав і свобод. Практично Європейський суд від початку виконував роль своєрідної наглядової інстанції щодо правозастосовних органів держав-учасниць. Зокрема, стало предметом широкої дискусії визначення конкретного змісту принципу “необхідності в демократичному суспільстві”, викладеного в ч. 2 ст. 10 Європейської конвенції з прав людини. В рамках цього тлумачення Європейський суд взяв до уваги національні особливості держав-членів конвенції, це сприйняття ґрунтувалося на так званій доктрині “межі оцінювання” (*margin of appreciation*), яка надавала державам-учасницям можливість для широкого розсуду при тлумаченні чи застосуванні окремих норм Конвенції. Такий підхід є частиною загальної тенденції, яку П. М. Рабінович визначає як “урізноманітнювання конкретного змісту й обсягу прав людини залежно від того, в якій країні вони мають реалізовуватись”¹⁰¹.

У 1988 р. Європейський суд, керуючись уже створеними прецедентами застосування відповідних норм Конвенції, дав визначення критерію необхідності в демократичному суспільстві. Зокрема, стверджується: “Згідно з усталеним прецедентним правом Суду, поняття необхідності передбачає, що втручання відповідає нагальній суспільній потребі і, зокрема, відповідає встановленій законом меті, визначаючи втручання “необхідне у демократичному суспільстві”, Суд вра-

¹⁰¹ Рабінович П. М. Зміст і обсяг прав людини: глобальна уніфікація чи внутрішньодержавна диверсифікація? // Актуальні проблеми політики: Зб. наук. праць. – Вип. 13 – 14. – Одеса: Юрид. літ-ра, 2002. – С. 42.

ховуватиме, що договірним державам відведено певні межі для свободи розсуду”¹⁰².

Разом з тим зазначається, що розгляд справи що провадиться Судом, по-перше, “не обмежується з’ясуванням того, чи держава-відповідач здійснювала свою свободу розсуду розумно, обережно і сумлінно. По-друге, під час здійснення своїх наглядових повноважень Суд може не обмежувати себе окремим розглядом оскаржених рішень, а має підійти до них з огляду на справу в цілому; він повинен з’ясувати, чи аргументи наведені на виправдання втручання, про яке йдеться, “доречні й достатні”¹⁰³.

Практично, за духом Конвенції і практики Європейського суду, можна розглядати обмеження реалізації інформаційних прав і свобод з боку держави як певне правопорушення, яке є цілком виправданим за наявності тих обставин, які у вітчизняному праві мають назву “крайньої необхідності”. Тобто обставин, за яких шкода від суспільно небезпечних наслідків, які можуть настати у зв’язку з реалізацією відповідних прав у сфері інформації, є значно більшою, ніж шкода від обмеження реалізації подібних прав. Тобто йдеться “про з’ясування серйозності втручання у закріплені в Конвенції права порівняно зі шкодою суспільним інтересам, яка може виникнути як наслідок неповного захисту зазначених інтересів”¹⁰⁴.

На жаль, у Конституції України¹⁰⁵ відтворюється лише перелік випадків і причин обмеження реалізації прав і свобод громадян у сфері інформації. Так, ст. 34 (гарантії свободи слова) передбачає можливість здійснення обмеження цього права:

- в інтересах національної безпеки і територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам;
- для охорони здоров’я населення;
- для захисту репутації або прав інших людей;
- для запобігання розголошенню інформації, одержаної конфіденційно,
- для підтримання авторитету і неупередженості правосуддя”.

¹⁰² Ollson v. Sweden, 11 E. H. H. R. 259.

¹⁰³ Ollson v. Sweden, 11 E. H. H. R. 259.

¹⁰⁴ Dadgeon v. United Kingdom, 4 E. H. H. R. 149. – p. 60

¹⁰⁵ Конституція України. Прийнята Верховною Радою України 28 червня 1996 р. // Відомості Верховної Ради. – 1996. – № 30. – Ст. 141.

У цьому аспекті значним кроком у врегулюванні балансу між правом на свободу слова та її обмеженням стало доповнення у 2003 р. Закону України “Про інформацію” ст. 47-1 “Звільнення від відповідальності”¹⁰⁶. Нормами цієї статті встановлено, що “ніхто не може бути притягнутий до відповідальності за висловлення оціночних суджень”, а самі “оціночні судження не підлягають спростуванню та доведенню їх правдивості”. Тим самим фактично визначено розмежування між фактами та оціночними судженнями, що відмежовує розповсюдження інформації, яке може бути обмежене, від висловлювання власних думок, яке обмеженням не підлягає.

У цій статті під *оціночним судженням* розуміється (за винятком образи чи наклепу) *висловлювання, які не містять фактичних даних, зокрема критика, оцінка дій, а також висловлювання, що не можуть бути витлумачені як такі, що містять фактичні дані, з огляду на характер використання мовних засобів, зокрема вживання гіпербол, алегорій, сатири*.

Відповідний баланс між правом на інформацію та її обмеженням, містить ч. 3 ст. 47-1 Закону України “Про інформацію”, згідно з якою “особа звільняється від відповідальності за розголошення інформації з обмеженим доступом, якщо суд встановить, що ця інформація є суспільно значимою”.

Ст. 32 Конституції (гарантії невтручання в особисте життя) допускає збирання конфіденційної інформації про особу без її згоди:

- в інтересах національної безпеки;
- економічного добробуту;
- прав людини.

Ст. 31 (таємниця кореспонденції) допускає встановлення винятків з метою:

- запобігти злочинам;
- з’ясувати істину під час розслідування кримінальної справи.

Загальною вимогою для всіх обмежень є їх установлення відповідно до закону, а ст. 31 містить також вимогу щодо встановлення обмеження лише судом.

Значною вадою механізму обмеження прав і свобод у сфері інформації, що встановлений Конституцією України, є відсутність важливого аспекту подібних обмежень – вичерпного переліку умов їх за-

¹⁰⁶ Про внесення змін до деяких законодавчих актів України з питань забезпечення та безперешкодної реалізації права людини на свободу слова: Закон України від 3 квітня 2003 р. № 676-IV. // Відомості Верховної Ради України. – 2003. – № 28. – Ст. 214.

стосовування. Лише в ст. 31 Конституції, що гарантує таємницю кореспонденції, визначається така умова, як неможливість одержати інформацію іншими засобами.

Ст. 64 Конституції також вказує лише на те, що конституційні права і свободи людини і громадянина не можуть бути обмежені, крім випадків, передбачених Конституцією України, знову ж таки не розкриваючи конкретних механізмів. І це вже не кажучи про можливість додаткових обмежень “в умовах воєнного або надзвичайного стану”, причому норми Конституції, які встановлюють інформаційні права людини, входять до переліку цих додаткових обмежень.

Таким чином, на рівні національного законодавства виникає значна прогалина в нормативно-правовому регулюванні механізму застосування подібних обмежень, що може відкрити простір для різних зловживань. І знову знаходить підтвердження теза про недостатнє забезпечення конституційних гарантій прав людини в Україні, без котрих будь-які передбачені Конституцією і законами права і свободи перетворюються на декларацію, яка, на жаль, все ще має підтвердження на практиці.

ГЛАВА 4.

ОСНОВНІ НАПРЯМИ РЕАЛІЗАЦІЇ ПРАВ І СВОБОД ЛЮДИНИ В СФЕРІ ІНФОРМАЦІЇ

Право громадян на звернення щодо надання інформації. Доступ до правової інформації. Доступ до екологічної інформації. Інформаційні права громадян як суб'єктів виборчого процесу. Захист персональних даних. Право на захист від негативного інформаційного впливу.

4. 1. Право на звернення щодо надання інформації

Важливою складовою права на свободу слова є право на вільний пошук і отримання інформації. Одним із способів отримання інформації є реалізація права на звернення, встановленого нормами ст. 40 Конституції України. В межах правовідносин, що виникають з приводу реалізації цієї норми суб'єктивному праву громадянина на подання індивідуальних або колективних звернень кореспондує обов'язок органів публічної влади дати обґрунтовану відповідь на такі звернення у встановлені законом строки.

Основною формою звернення щодо надання інформації є *запит* до органів державної влади та місцевого самоврядування, порядок подання й задоволення якого визначається Законом України “Про інформацію”¹⁰⁷ (ст. 32–37).

Закон виділяє два типи запитів про надання інформації:

- *інформаційний запит щодо доступу до офіційних документів* – звернення з вимогою про надання можливості ознайомитися з офіційними документами;
- *запит щодо надання письмової або усної інформації* – звернення з вимогою надати письмову або усну інформацію про діяльність органів законодавчої, виконавчої та судової влади України, їх посадових осіб з окремих питань.

Запит може бути індивідуальним або колективним. Право на подання запиту мають громадяни України, органи публічної влади, ор-

¹⁰⁷ Про інформацію: Закон України від 2 жовтня 1992 р. // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

ганізації і об'єднання громадян. Крім того, законодавство передбачає що іноземні громадяни також користуються правом на звернення.

Запит повинен обов'язково містити: прізвище, ім'я та по батькові запитувача, документ, письмову або усну інформацію про те, що його цікавить, та адресу, за якою він бажає одержати відповідь.

Надання можливості ознайомлення з офіційними документами передбачає право запитувача робити виписки з наданих офіційних документів, фотографувати їх, записувати текст на магнітну плівку, отримати за плату копію документу тощо.

Надання інформації про діяльність органів публічної влади та їх посадових осіб передбачає обов'язок службових осіб надавати таку інформацію письмово, усно, по телефону чи використовуючи публічні виступи своїх посадових осіб.

Законодавство встановлює граничні терміни:

- для вивчення запиту на предмет можливості його задоволення – десять календарних днів, протягом яких орган публічної влади повинен письмово повідомити запитувачеві про можливість або неможливість задоволення його запиту;
- для задоволення запиту – один місяць, якщо інше не передбачено законом.

У разі якщо запитувана інформація не підлягає наданню для ознайомлення, орган публічної влади має право відмовити у задоволенні запиту. Відмова дається тільки в письмовій формі із зазначенням: посадової особи, що ухвалила рішення про відмову, дати та мотивованих підстав відмови, роз'яснення порядку оскарження прийнятого рішення.

За неможливості надання запитуваної інформації у передбачений законом строк орган публічної влади має право повідомити про відстрочення задоволення запиту. Про відстрочення повідомляють у письмовій формі із зазначенням: посадової особи, яка відмовляє у задоволенні запиту у визначений місячний термін; дати надсилання або видачі повідомлення про відстрочення; причини, з яких запитуваний документ не може бути виданий у встановлений цим Законом термін; термін, за який буде задоволено запит, роз'яснення порядку оскарження прийнятого рішення.

Запитувачі повинні повністю або частково відшкодувати витрати, пов'язані з виконанням запитів щодо доступу до офіційних документів та наданням письмової інформації, в т. ч. виготовлення копій офі-

ційних документів, але в розмірі, що не перевищує реальних витрат, пов'язаних з виконанням запитів. Не підлягає оплаті робота з пошуку офіційних документів.

Законодавство передбачає два способи оскарження відмови та відстрочення у задоволенні запиту – в судовому порядку або оскарженням в органи влади вищого рівня.

Оскарження до органів влади вищого рівня здійснюється на підставі та в порядку передбаченому Законом України “Про звернення громадян”¹⁰⁸ і в порядку, визначеному цим Законом та Інструкцією з діловодства за зверненнями громадян в органах державної влади і місцевого самоврядування, об'єднаннях громадян, на підприємствах, в установах, організаціях незалежно від форм власності, в засобах масової інформації¹⁰⁹.

4. 2. Доступ до правової інформації

Окремим аспектом реалізації загального права на інформацію слід розглядати право на доступ до правової інформації, корені якого можна знайти у сформульованому римськими юристами принципі “незнання закону не звільняє від відповідальності”. Разом з тим такий принцип вимагає від держави надати можливість кожній особі ознайомитися зі змістом законів.

Право на доступ до правової інформації ґрунтується на нормах ст. 57 Конституції, згідно з якими “кожному гарантується право знати свої права і обов'язки”¹¹⁰.

Ст. 57 Конституції містить два окремих механізми, які повинні забезпечувати це право.

По-перше, нормами ч. 2 ст. 57 Конституції встановлюється позитивне зобов'язання для органів публічної влади, згідно з яким закони та інші нормативно-правові акти, що визначають права і обов'язки громадян, мають бути доведені до відома населення в порядку, встановленому законом.

¹⁰⁸ Про звернення громадян: Закон України від 2 жовтня 1996 р. № 393/96-ВР // Відомості Верховної Ради. – 1996. – № 47. – Ст. 256.

¹⁰⁹ Про затвердження Інструкції з діловодства за зверненнями громадян в органах державної влади і місцевого самоврядування, об'єднаннях громадян, на підприємстві, в установі, організації незалежно від форм власності, в засоби масової інформації: Постанова Кабінету Міністрів України від 14 квітня 1997 р. № 348.

¹¹⁰ Конституція України. Прийнята Верховною Радою України 28 червня 1996 р. // Відомості Верховної Ради. – 1996. – № 30. – Ст. 141.

По-друге, (ч. 3. ст. 57 Конституції), встановлюється правило, згідно з яким згадані в попередній частині нормативно-правові акти, які не були доведені до відома населення у порядку, встановленому законом, є нечинними.

Слід зазначити, що відповідні положення стосуються всіх законодавчих актів і тих нормативно-правових актів, що *встановлюють права і обов'язки громадян*. Таким чином вони не поширюються на деякі нормативно-правові акти органів публічної влади, які не мають загального значення або нормативного характеру.

Специфічною особливістю права на доступ до правової інформації можна назвати його абсолютність. Тобто не допускаються будь-які обмеження названого права ані за звичайних умов, ані за умов воєнного або надзвичайного стану, оскільки, згідно зі ст. 64 Конституції, право знати свої права і обов'язки віднесено до переліку прав, які не можуть бути обмежені ні за яких обставин.

Безпосередньо порядок публікації названих законів і нормативно-правових актів регулюється Регламентом Верховної Ради¹¹¹ та Указом Президента України “Про порядок офіційного оприлюднення нормативно-правових актів та набрання ними чинності”¹¹².

Згідно зі ст. 134 Регламенту Верховної Ради, підписані Президентом України закони й закони, які офіційно оприлюднені Головою Верховної Ради України, публікуються в газеті “Голос України” та у “Відомостях Верховної Ради України”, що вважається їх офіційною публікацією. Ці самі видання публікують постанови й інші акти Верховної Ради, причому апарат Верховної Ради зобов'язаний передати їх для публікації не пізніше наступного дня після їх підписання Головою Верховної Ради.

Оригінал нормативно-правового акту зберігається в апараті Верховної Ради. Оригіналами вважаються лише:

- підписаний Президентом України закон;
- підписані Головою Верховної Ради України постанови та інші акти Верховної Ради.

Всі інші примірники закону, постанови та інших актів Верховної Ради є копіями.

¹¹¹ Про Регламент Верховної Ради України: Постанова Верховної Ради України від 16 березня 2006 р. № 3547-IV // Відомості Верховної Ради України. – 2006. – № 23, № 24 – 25. – Ст. 202.

¹¹² Про порядок офіційного оприлюднення нормативно-правових актів та набрання ними чинності: Указ Президента України. Від 10 червня 1997 р. № 503/97. (В редакції Указу Президента України №1235/98 Від 10 листопада 1998 р.)

Ч. 3 ст. 134 Регламенту Верховної Ради передбачає, що у разі виявлення невідповідності опублікованого закону, постанови чи іншого акта Верховної Ради його оригіналу, не пізніш як через десять днів з дня виявлення невідповідності публікується в газеті “Голос України” та в черговому номері “Відомостей Верховної Ради України” уточнений текст цього нормативно-правового акта.

Крім того, ст. 198 Регламенту Верховної Ради передбачає, що міжнародні договори України, згода на обов’язковість яких законом надана Верховною Радою, публікуються українською мовою в офіційних друкованих виданнях України.

Згаданий Указ Президента (ст. 1) встановлює строк *п’ятнадцять днів з моменту прийняття і підписання*, протягом якого закони України, інші акти Верховної Ради, акти Президента України та Кабінету Міністрів підлягають оприлюдненню. Оприлюднення цих нормативно-правових актів здійснюється державною мовою в офіційних виданнях.

Слід зазначити, що цей Указ вводить певну класифікацію офіційних видань, відповідно до органів державної влади, чиї акти можуть публікуватися у них. Так, офіційними друкованими виданнями, в яких здійснюється оприлюднення будь-яких нормативно-правових актів, є:

- “Офіційний вісник України”,
- Газета “Урядовий Кур’єр”.

Офіційними друкованими виданнями, в яких здійснюється офіційне оприлюднення виключно законів та інших актів Верховної Ради України є:

- газета “Голос України”;
- “Відомості Верховної Ради України”.

Офіційним друкованим виданням, в якому здійснюється офіційне оприлюднення законів, актів Президента України, є

- інформаційний бюлетень “Офіційний вісник Президента України”.

В окремих випадках акти Верховної Ради України, Президента України, Кабінету Міністрів України можуть бути офіційно оприлюднені через телебачення і радіо.

Вимоги до обов’язкової публікації не поширюються лише на акти Верховної Ради України, Президента України, Кабінету Міністрів

України, які не мають загального значення чи нормативного характеру, можуть не публікуватися за рішенням відповідного органу. Ці акти оприлюднюються шляхом надіслання органам публічної влади та доведення до відома осіб, яких вони стосуються.

З гарантуванням права на доступ до правої інформації пов'язаний і механізм набрання чинності нормативно-правовими актами. Так, для *нормативно-правових актів Верховної ради України та Президента України* встановлено загальне правило щодо набрання чинності через 10 днів з дня офіційного оприлюднення, якщо інше не передбачено самими актами, але не раніше дня їх опублікування в офіційному друкованому виданні.

Для *нормативно-правових актів Кабінету Міністрів* – з моменту їх прийняття, якщо більш пізній строк набрання ними чинності не передбачено в цих актах, за винятком актів, які визначають права і обов'язки громадян, що набирають чинності не раніше дня їх опублікування в офіційних друкованих виданнях.

Для *неопублікованих актів Верховної Ради України і Президента України* з моменту їх одержання відповідними органами державної влади та місцевого самоврядування, якщо органом, що їх видав, не встановлено інший строк набрання ними чинності, за винятком актів щодо призначення на посади і звільнення з посад, що набирають чинності з моменту прийняття.

Окреме положення, що ґрунтується на міжнародно-правових стандартах, стосується *законів, які вносять зміни до Митного тарифу України та інших нормативно-правових актів з питань митної справи* котрі набирають чинності через 45 днів з дня їх офіційного опублікування, якщо інше не передбачено самим актом, але не раніше дня їх офіційного оприлюднення.

Важливим джерелом правової інформації є Єдиний державний реєстр нормативних актів (Реєстр), який є автоматизованою системою збирання, накопичення та опрацювання актів законодавства, що складається з еталонного, страхового, робочого, інформаційного фондів та окремого розділу¹¹³.

Уведення цього Реєстру здійснює Міністерство юстиції України, а безпосереднє забезпечення функціонування Реєстру та надання інформації покладено на визначених ним адміністраторів реєстру.

¹¹³ Про затвердження Порядку ведення Єдиного державного реєстру нормативно-правових актів та користування ним: Постанова Кабінету Міністрів України від 23 квітня 2001 р. № 376.

Реєстр створено з метою:

- забезпечення додержання єдиних принципів ідентифікації нормативно-правових актів та ведення їх державного обліку в межах інформаційного простору України;
- створення фонду та підтримання в контрольному стані нормативно-правових актів, надання інформації про них;
- забезпечення в межах, визначених законодавством, доступності, гласності та відкритості правової інформації для користувачів.

Включенню до Реєстру підлягають:

- нормативно-правові акти, видані починаючи з дня прийняття Акта проголошення незалежності України (24 серпня 1991 р.) – чинні, опубліковані та неопубліковані, у т. ч. з обмежувальними грифами (включаються до окремого розділу), що були видані центральними органами державної влади, а також міжнародні договори України;
- нормативно-правові акти, видані до прийняття Акта проголошення незалежності України (24 серпня 1991 р.), що не втратили чинності та не суперечать законодавству України;
- тимчасові нормативно-правові акти з терміном дії рік і більше та з терміном дії менше року в разі наступного його продовження.

Юридичні і фізичні особи можуть одержати копії еталонних текстів нормативно-правових актів з інформаційного фонду Реєстру на електронних чи паперових носіях, шляхом звернення до адміністратора Реєстру або безпосереднього санкціонованого доступу до інформаційного фонду Реєстру. Надання інформації здійснюється на підставі запиту або договору згідно з Інструкцією про порядок та умови одержання інформації з інформаційного фонду Єдиного державного реєстру нормативно-правових актів¹¹⁴.

Запит про одержання інформації з інформаційного фонду розглядається і задовольняється Адміністратором Реєстру в термін не більше десяти робочих днів з дня надходження коштів від користувача Реєстру в рахунок оплати послуг з надання інформації відповідно до цього запиту, а запити, які не потребують додаткового вивчення – невідкладно, але не пізніше п'яти робочих днів з дня надходження коштів.

¹¹⁴ Про затвердження Інструкції про порядок та умови одержання інформації з інформаційного фонду Єдиного державного реєстру нормативно-правових актів: Наказ Міністерства юстиції України від 26 червня 2002 р. № 57/5.

Слід зазначити, що можливе також розширювальне тлумачення права громадян на доступ до правової інформації як можливості не лише ознайомитися з текстами законів, а й отримувати певні правові знання, необхідні для того, щоб бути повноправним членом демократичного суспільства. Наприклад, досить поширеною є думка щодо необхідності здійснення державою заходів для поширення правових знань та правової пропаганди серед населення.

Нині надання правової допомоги, в т. ч. й коштом держави, здійснює насамперед адвокатура України. Крім того, поширення правових знань, правової інформації, надання безкоштовних консультацій з правових питань вирішується зусиллями громадських організацій.

Нарешті, згідно з Наказом Міністерства юстиції України¹¹⁵, передбачено функціонування *правових громадських приймалень*, які створюються для надання місцевими органами виконавчої влади, територіальними підрозділами центральних органів виконавчої влади безоплатної правової допомоги малозабезпеченим особам.

Основними видами правової допомоги, які здійснює правова громадська приймальня, є:

- надання консультацій і роз'яснень з правових питань;
- допомога в складанні документів правового характеру (звернень громадян, окремих процесуальних документів).

Важливим засобом правової інформації є і неофіційні її джерела. Зокрема, згідно зі ст. 22 Закону України “Про інформацію”, до таких джерел належать: повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань.

Передбачається також, що з метою забезпечення доступу до законодавчих та інших нормативних актів всім громадянам держава забезпечує видання цих актів масовими тиражами у найкоротші строки після набрання ними чинності.

4. 3. Доступ до екологічної інформації

Екологічна інформація є одним із специфічних видів інформації, право доступу до якої забезпечується окремими правовими механізмами, що встановлені згідно з міжнародно-правовими стандартами. Це пов'язано з тим, що нині питання екологічної безпеки є не лише

¹¹⁵ Наказ Міністерства юстиції України “Про затвердження Типового положення про правову громадську приймальню” від 15 червня 2005 р. № 61/5.

внутрішньодержавними, а й загальносвітовими. Причому питання доступу до екологічної інформації виступає окремим аспектом екологічної безпеки. Право на доступ до екологічної інформації можна розглядати як *право і необхідність людини (громадянина) бути достатньо поінформованою про можливі загрози та наслідки, зумовлені станом навколишнього середовища для здійснення свідомого вибору своєї поведінки*.

Специфіку цього права на інформацію визначено в ч. 2. ст. 50 Конституції України, вона є частиною закріпленого нормами цієї статті права на безпечне для життя і здоров'я довкілля та на відшкодування завданої порушенням цього права шкоди.

Право на цей вид інформації, за ч. 2 ст. 50 Конституції, складається з трьох елементів:

- 1) це право вільного доступу до інформації про стан довкілля, про якість харчових продуктів і предметів побуту;
- 2) це право поширювати таку інформацію;
- 3) норма, за якою така інформація ніким не може бути засекречена.

Специфікою права на екологічну інформацію, за якою вона відрізняє його від загальних інформаційних прав, є саме третій елемент, який виключається за звичайних умов введення обмежень щодо цієї інформації. (Крім випадків воєнного або надзвичайного стану, передбачених ст. 64).

У міжнародних актах право на отримання екологічної інформації, зокрема, передбачено Конвенцією про доступ до інформації, участь громадськості в процесі прийняття рішень і доступ до правосуддя з питань, що стосуються довкілля¹¹⁶.

Безпосередньо питання доступу до екологічної інформації регулюються ст. 4 цієї Конвенції. У ній зазначено, зокрема, що державні органи сторін-учасниць у відповідь на запит про надання екологічної інформації повинні надавати громадськості таку інформацію в рамках національного законодавства, включаючи, при необхідності і можливості, копії фактичних документів, які містять або охоплюють таку інформацію. Екологічна інформація надається в максимально стислі строки. Граничний строк відповіді на запит – один місяць,

¹¹⁶ Конвенція про доступ до інформації, участь громадськості в процесі прийняття рішень та доступ до правосуддя з питань, що стосуються довкілля. Від 28 червня 1998 р. (Ратифіковано Законом України № 832-XIV від 6 липня 1999 р.) // Відомості Верховної Ради України. – 1999. – № 34. – Ст. 296.

але у випадку значних обсягів та складності відповідної інформації цей термін може бути продовжено до двох місяців, про що інформується подавець заяви.

Пунктами 3 та 4 ст. 4 Конвенції також передбачено перелік випадків, коли в наданні такої інформації може бути відмовлено. Це можливо, якщо: державний орган, до якого було направлено запит, не має у своєму розпорядженні відповідної екологічної інформації; запит є очевидно необґрунтованим або сформульованим в надто загальному вигляді; або запит стосується матеріалів, що перебувають на завершальній стадії їх підготовки, або стосується внутрішнього інформаційного обміну міждержавними органами, коли такий виняток передбачається національним законодавством чи практикою, що склалася, при цьому враховується зацікавленість громадськості в розкритті такої інформації.

Крім того, в наданні екологічної інформації може бути відмовлено, якщо надання такої інформації може негативно вплинути на: конфіденційність діяльності державних органів, міжнародні стосунки, національну оборону або державну безпеку, відправлення правосуддя, конфіденційність комерційної та промислової інформації, права інтелектуальної власності, конфіденційність особистих даних, інтереси третьої сторони, яка надала інформацію; навколишнє середовище.

Для того, щоб запобігти зловживанням обмеженням права на доступ до екологічної інформації, передбачається (п. 6), що у випадках, коли інформація, що не підлягає оприлюдненню, може бути відокремлена від решти інформації без шкоди для конфіденційності інформації, яка не підлягає оприлюдненню, державні органи надаватимуть цю решту екологічної інформації.

Якщо у наданні інформації відмовлено, у цій відмові повинні бути зазначені її причини і наведена відповідна інформація про доступ до процедур перегляду прийнятого рішення.

Як уже зазначалося, згідно з Конституцією України, екологічна інформація ніким не може бути засекречена. Таким чином, можна стверджувати, що саме регламентація права на екологічну інформацію є чи не єдиною сферою інформаційних прав, у якій національне українське законодавство пішло навіть далі, ніж вимагають міжнародно-правові акти з цих питань.

Щодо деталізації права на екологічну інформацію, то вона існує в нормах низки законодавчих актів. Так, згідно зі ст. 25 Закону Украї-

ни “Про захист навколишнього природного середовища”, основними джерелами екологічної інформації є: дані моніторингу довкілля, кадастрів природних ресурсів, реєстри, автоматизовані бази даних, архіви, а також довідки, що видаються уповноваженими на те органами державної влади, органами місцевого самоврядування, громадськими організаціями, окремими посадовими особами.

Ст. 25-1 цього Закону визначає обов’язок органів державної влади та органів місцевого самоврядування в межах їх повноважень здійснювати *екологічне інформаційне забезпечення* шляхом:

- підготовки Міністерством охорони навколишнього природного середовища України і подання на розгляд Верховної Ради України щорічної Національної доповіді про стан навколишнього природного середовища в Україні, а після її розгляду Верховною Радою України – опублікування окремим виданням та розміщення в Інтернет;
- щорічного інформування Радою міністрів Автономної Республіки Крим, обласними державними адміністраціями, Київською та Севастопольською міськими державними адміністраціями відповідних рад та населення про стан навколишнього природного середовища відповідних територій;
- систематичного інформування населення через засоби масової інформації про стан навколишнього природного середовища, динаміку його змін, джерела забруднення, розміщення відходів чи іншої зміни навколишнього природного середовища і характер впливу екологічних факторів на здоров’я людей;
- негайного інформування про надзвичайні екологічні ситуації;
- передачі інформації, отриманої в результаті проведення моніторингу довкілля, каналами інформаційних зв’язків органам, уповноваженим приймати рішення щодо отриманої інформації;
- забезпечення вільного доступу до екологічної інформації, яка не становить державної таємниці і міститься у списках, реєстрах, архівах та інших джерелах.

Безпосередньо порядок надання екологічної інформації та участі громадськості у прийнятті рішень з питань навколишнього середовища визначається згідно з нормативно-правовими актами з охорони навколишнього природного середовища України:

- Положенням про порядок надання екологічної інформації¹¹⁷,
- Положенням про щоквартальне інформування населення через ЗМІ про об'єкти, які є найбільшими забруднювачами навколишнього природного середовища¹¹⁸,
- Положенням про участь громадськості у прийнятті рішень у сфері охорони довкілля¹¹⁹.

Окремо слід сказати про положення Закону України “Про зону надзвичайної екологічної ситуації”, які регулюють порядок інформування населення з приводу надзвичайних екологічних ситуацій. Згідно зі ст. 4 цього Закону, серед основних принципів регулювання правового режиму в зоні надзвичайної екологічної ситуації називається “забезпечення населення достовірною інформацією про стан довкілля, можливу загрозу для життя та здоров'я людей і про виконання заходів, спрямованих на нормалізацію екологічного стану”¹²⁰. Цим Законом (ст. 6) передбачено також, що указ Президента України про оголошення окремої місцевості зоною надзвичайної екологічної ситуації доводиться до відома населення через засоби масової інформації та систему оповіщення цивільної оборони.

Зазначимо, що Конвенція “Про доступ до інформації, участь громадськості в процесі прийняття рішень та доступ до правосуддя з питань, що стосуються довкілля” (ст. 5), вимагає насамперед створення механізмів забезпечення широкої громадськості екологічною інформацією. Відповідно до її вимог, потрібно, щоб:

- державні органи мали у своєму розпорядженні екологічну інформацію та постійно поновлювали її;
- було створено обов'язкові системи забезпечення належного надходження в державні органи екологічної інформації;
- у випадках, що становлять безпосередню загрозу для здоров'я людини або навколишнього середовища, які виникають в результаті людської діяльності або є наслідком природних явищ, вся інформація, яка могла би дозволити громадськості вжити

¹¹⁷ Про затвердження Положення про порядок надання екологічної інформації: Наказ Мінприроди України від 18 грудня 2003 р. № 169.

¹¹⁸ Про затвердження Положення про щоквартальне інформування населення через ЗМІ про об'єкти, які є найбільшими забруднювачами навколишнього природного середовища: Наказ Мінприроди України від 1 листопада 2005 р. № 397.

¹¹⁹ Про затвердження Положення про участь громадськості у прийнятті рішень у сфері охорони довкілля: Наказ Мінприроди України від 18 грудня 2003 р. № 168.

¹²⁰ Про зону надзвичайної екологічної ситуації: Закон України від 13 липня 2000 р. № 1908-III // Відомості Верховної Ради. – 2000. – № 42. – Ст. 348.

заходів із запобігання або зменшення шкоди, яка може стати наслідком такої загрози і яка є у розпорядженні державного органу, негайно поширювалася б серед членів громадськості, яких потенційно торкається загроза.

Конвенція покладає саме на державу та її органи забезпечення права на доступ до екологічної інформації, для чого передбачається здійснення таких заходів:

- забезпечення у межах національного законодавства прозорості та доступності процедури надання громадськості екологічної інформації;
- забезпечення поступового збільшення обсягу екологічної інформації в електронних базах даних, які є легкодоступними для широкого загалу громадськості через публічні мережі зв'язку;
- регулярна (не рідше ніж через три або чотири роки) публікація і поширення національних звітів про стан навколишнього середовища;
- поширення інформації про національні і міжнародні нормативно-правові акти з екологічних питань;
- заохочення діячів, чия діяльність справляє суттєвий вплив на навколишнє середовище;
- розробка механізмів з метою забезпечення громадськості достатньою інформацією стосовно продуктів таким чином, щоб надавати можливість споживачам робити екологічно обгрунтований вибір.

Останнє положення, щодо надання можливості робити “екологічно обгрунтований вибір”, найбільшою мірою відображає сутність і мету забезпечення права людини і громадянина на доступ до екологічної інформації.

4. 4. Інформаційні права громадян як суб'єктів виборчого процесу

Права і свободи людини в галузі інформації, як уже зазначалося, належать до категорії прав людини першого покоління – громадських та політичних прав. Тому цілком логічним є те, що їх реалізація невід'ємно пов'язана насамперед із політичними процесами. В межах цих процесів у державі й суспільстві складається так звана система політичної комунікації, в основі якої лежать інформаційні

відносини. “Політична комунікація є соціальною взаємодією через повідомлення, яка стосується управління і здійснення влади в суспільстві. Така соціальна взаємодія відбувається у багатьох формах: від дебатів за кухлем пива у барі до випуску партійних буклетів і виступів політиків на сесіях і зібраннях. ... У сучасних демократичних суспільствах процес політичної комунікації майже весь реалізується через засоби масової інформації”¹²¹. Основним завданням політичної комунікації є забезпечення громадянам можливості вивчити суспільно значущі проблеми, скласти власну думку про них та сформулювати громадську думку, яка може впливати на діяльність органів публічної влади.

У питаннях правового регулювання інформаційних відносин, що виникають у межах процесу політичної комунікації, можна виділити два аспекти:

1) поточна політична комунікація, котра, як зазначалося, може здійснюватися в різних формах. Інформаційні відносини, що виникають з приводу поточної політичної комунікації, регулюються за загальними нормами і правилами а реалізація права громадян на свободу слова зазнає мінімальних обмежень, що визначені Конституцією та законодавством;

2) політична комунікація, що відбувається в межах здійснення громадянами безпосередньої демократії, насамперед у формі виборів та референдумів. Відповідні інформаційні відносини насамперед пов’язані “із формуванням активного та свідомого вибору громадян у процесі демократичного волевиявлення”¹²².

Інформаційні відносини, пов’язані з проведенням виборів та референдумів, завжди були важливим елементом впливу як на їх перебіг, так і на їх результати. Через це законодавство застосовує додаткові правила реалізації інформаційних прав і свобод громадян в умовах виборчих кампаній, метою яких є запобігання зловживанням, які б могли зашкодити формуванню свідомого вибору. Відповідні особливі норми, що регулюють інформаційні відносини в процесі здійснення безпосередньої демократії, містяться насамперед у виборчому законодавстві.

¹²¹ Крос К., Гакет Р. Політична комунікація і висвітлення новин у демократичних суспільствах. Перспективи конкуренції. – К.: Основи, 2000. – С. 10.

¹²² Конституційно-правові форми безпосередньої демократії в Україні: проблеми теорії і практики. До 10-ї річниці незалежності України. – К.: Інститут держави і права ім. В. М. Корецького НАН України, 2001. – с. 249 – 250.

Для більш чіткого аналізу існуючих загроз цьому процесу важливо класифікувати відносини, пов'язані з електоральною інформацією, адже ні ця інформація, ні ці відносини не є однорідними.

Серед правових відносин, що виникають із приводу реалізації прямого народовладдя, зазвичай виділяють такі основні групи:

1) відносини, пов'язані із забезпеченням виборцям і учасникам виборів та референдумів поінформованості (розширення кола об'єктивних знань) з питань виборчого законодавства, законодавства про референдуми; з проблем державотворення, місцевого самоврядування з метою розвитку політико-правової культури громадян, підвищення їхньої правосвідомості як реальних і потенційних учасників названих процесів;

2) відносини, пов'язані з інформаційним забезпеченням проведення виборів і референдумів на всіх основних стадіях. Серед них – підвищення професійних знань організаторів виборів та референдумів (членів виборчих комісій та комісій з референдумів, органів, що утворюють ці комісії) з метою забезпечення кваліфікованого проведення відповідних заходів; забезпечення правової поінформованості кандидатів та їх довірених осіб з питань висування та реєстрації кандидатів у депутати, правил ведення передвиборної агітації, встановлених чинним законодавством, спілкування з виборцями, представниками засобів масової інформації та ін. Особливо слід заважити на інформаційні відносини пов'язані зі створенням іміджу кандидата або політичного об'єднання (політична реклама зокрема) ¹²³

Ще одним важливим аспектом можна назвати відносини, пов'язані з процесом оброблення, передавання та оприлюднення результатів виборів та референдумів. Тобто відносини пов'язані з наданням юридичного статусу результатам народного волевиявлення, адже вони також пов'язані з процесами оброблення і передавання інформації, до яких встановлюються підвищенні вимоги щодо достовірності та повноти такої інформації.

Більшість дій, що формують негативний, деструктивний вплив на інформаційні відносини під час виборів, охоплюються широко вживаними останнім часом термінами “брудні виборчі технології” та “чорний PR”. Але помилкою було б вважати це сучасними винаходами. Пропагандистсько-ідеологічні засади є найбільш давньою опорою

¹²³ Конституційно-правові форми безпосередньої демократії в Україні: проблеми теорії і практики. До 10-ї річниці незалежності України. – К. : Інститут держави і права ім. В. М. Корецького НАН України, 2001. – С. 249 – 250.

державної влади, адже вони свого часу стали одним із факторів формування цього феномену. Достатньо згадати різні теологічні концепції, що обстоювали “божественне” походження влади. Протягом тривалого часу ідеологічні засади постійно змінювалися, але основне їх завдання залишалося однаковим – пояснити народові, чому саме ця влада повинна існувати, чому саме ці особи або політичні сили повинні управляти суспільством. Своє оригінальне бачення феномену державної влади було запропоноване свого часу М. Бердяєвим, який зазначав, що: “Державна влада може дуже раціонально правити народом, але саме джерело влади є ірраціональним. Вдача людей влади полягає у здатності до навіювання. Володарює той, хто втягує народні маси в гіпнотичний стан. Пропаганда відіграє тут таку колосальну роль, вона є вульгарною формою гіпнотизування. І якби люди мали здатність не піддаватися гіпнозу, то невідомо яка влада могла б втриматися”¹²⁴.

Зазначимо, що події виборчих кампаній останніми роками значно активізували процес формування законодавчого регулювання інформаційних процесів, що відбуваються під час виборів, особливо в тому, що стосується передвиборної агітації, інформаційного забезпечення діяльності виборчих комісій тощо. А це, в свою чергу, значно підвищило дотримання відповідних інформаційних прав і свобод громадян.

Основна гарантія дотримання прав і свобод громадян у процесі здійснення безпосередньої демократії є норма ч. 2. ст. 71 Конституції України, згідно з якою “кожному гарантується вільне волевиявлення”¹²⁵. Таким чином, порушення виборчого законодавства є актом обмеження права на вільне волевиявлення.

На жаль, в Україні сформувалася система таких порушень, найбільш поширені з яких, за даними Комітету виборців України, є:

- масові порушення заборони на агітацію;
- використання службового становища керівниками органів місцевої влади та місцевого самоврядування;
- адміністративний тиск на суб’єктів виборчого процесу і ЗМІ;
- агітація з використанням безкоштовного або за зниженими цінами надання товарів та послуг;
- використання брудних передвиборних технологій (чорний PR);

¹²⁴ Бердяев Н. Судьба России. – М., 1990. – С. 268.

¹²⁵ Конституція України. Прийнята Верховною Радою України 28 червня 1996 р. // Відомості Верховної Ради. – 1996. – № 30. – Ст. 141.

- розповсюдження інформації (агітація) від імені конкурента, порушення процедури формування виборчих комісій, факти насильства щодо учасників виборчого процесу;
- пряма агітація з боку посадових осіб¹²⁶.

Значна частина перелічених порушень виборчого законодавства пов'язана з протиправним втручанням в інформаційні відносини, що виникають під час виборчої кампанії, насамперед у межах передвиборної агітації. Відповідно виборче законодавство містить низку норм, які регулюють інформаційні відносини під час проведення передвиборної агітації, формують механізми забезпечення однакових умов та неупередженого формування громадської думки.

Так, у Законі України “Про вибори народних депутатів України” (ч. 2. ст. 10) визначено такі засади виборчого процесу:

- законності та заборони незаконного втручання будь-кого у цей процес;
- свободи передвиборної агітації, рівних можливостей доступу до засобів масової інформації;

Слід зазначити, що в 2005 р. нарешті у вітчизняному законодавстві було сформульовано визначення *передвиборної агітації*, як “здійснення будь-якої діяльності з метою спонукання виборців голосувати за або проти певного суб'єкта виборчого процесу”. Законодавство виділяє форми передвиборної агітації, щодо яких устанавлюються особливі правила проведення або використання, а саме:

- проведення масових заходів (мітинги, концерти, збори);
- використання друкованих та електронних ЗМІ;
- розповсюдження та розміщення на носіях зовнішньої реклами друкованих матеріалів передвиборної агітації;
- публічні заклики.

Законом дозволяється проведення агітації у будь-яких формах, що не суперечать Конституції та законодавству України.

Визначена законодавством система заборон і обмежень щодо ведення передвиборної агітації має на меті забезпечити демократичність і законність, рівні умови для всіх кандидатів, запобігання застосуванню “брудних виборчих технологій”, тиску на виборців з боку органів публічної влади, іноземному впливу на перебіг виборчої кампанії та ін.

¹²⁶ Див.: Звіт про порушення під час виборчої кампанії по виборах народних депутатів України 2002 року протягом січня 2002 р. за підсумками моніторингу КВУ / Вибори 2002 в Україні: перемога криміналітету чи демократичних сил. – К., 2002. – С. 225–234.

Якщо узагальнити відповідні норми, встановлені виборчим законодавством (щодо виборів Президента України, народних депутатів України), то можна сказати, що обмеження у веденні передвиборної агітації стосуються:

- суб'єктів передвиборної агітації;
- місць проведення заходів передвиборної агітації;
- форм, засобів та змісту передвиборної агітації;
- строків і термінів передвиборної агітації та окремих її форм.

Насамперед слід виділити *суб'єктів, яким забороняється участь у передвиборній агітації*. Це:

- іноземці та особи без громадянства;
- органи виконавчої влади та місцевого самоврядування;
- посадові і службові особи органів виконавчої влади та місцевого самоврядування;
- члени виборчих комісій під час виконання своїх обов'язків членів виборчих комісій;
- зарубіжні засоби масової інформації, що діють на території України.

Наступна група обмежень стосується *місць здійснення передвиборної агітації*, в яких проведення заходів передвиборної агітації обмежено або заборонено, а саме:

- військових частин (формувань);
- установах кримінально-виконавчої системи.

Певні обмеження визначено щодо *форм, методів та змісту передвиборчої агітації*. Зокрема, забороняється поширення в будь-якій формі матеріалів, що містять заклики до ліквідації незалежності України, зміни конституційного ладу насильницьким шляхом, порушення суверенітету й територіальної цілісності держави, підриву її безпеки, незаконного захоплення державної влади, пропаганду війни, насильства та розпалювання міжетнічної, расової, національної, релігійної ворожнечі, посягання на права і свободи людини, здоров'я населення.

Друкованим та електронним ЗМІ забороняється у своїх матеріалах і передачах, не обумовлених угодами, що укладені відповідно до виборчого законодавства, агітувати за або проти партій (блоків), висунутих ними кандидатів чи поширювати інформацію, яка має ознаки політичної реклами, а так само поширювати будь-яку інформацію з метою спонукання виборців голосувати за або проти певного суб'єкта виборчого процесу.

Деякі характерні обмеження стосуються політичної реклами. Зокрема, забороняється:

- розміщення політичної реклами в одному блоці з комерційною чи соціальною рекламою;
- введення передвиборних агітаційних матеріалів до інформаційних теле- і радіопрограм (випусків новин);
- розповсюдження завідомо недостовірних або наклепницьких відомостей про партію (блок) або кандидата — суб'єкта виборчого процесу чи про кандидата в депутати;
- виготовлення та розповсюдження друкованих передвиборних агітаційних матеріалів, що не містять відомостей про установу, яка здійснила друк, їх тираж, інформацію про осіб, відповідальних за випуск.

Останні обмеження спрямовані насамперед на забезпечення виборцям можливості відстежувати матеріали передвиборної агітації та адекватно їх сприймати.

До заборонених форм передвиборної агітації належать також надання виборцям грошей чи безоплатно або на пільгових умовах товарів, послуг, робіт, цінних паперів, кредитів, лотерей.

Певні обмеження, визначено також і щодо *строків проведення заходів передвиборної агітації*. Ці строки установлюють з урахуванням дати і видів інформації, яка має або може впливати, на перебіг виборчої кампанії та результати волевиявлення виборців:

1) протягом останніх п'ятнадцяти днів перед днем виборів засобам масової інформації заборонено поширювати інформацію про результати опитувань громадської думки;

2) за два дні, починаючи з 24. 00 останньої п'ятниці перед днем виборів, закінчується передвиборна агітація, що передбачає:

- закінчення проведення “активної агітації”, до якої віднесено: публікацію агітаційних матеріалів у засобах масової інформації, розповсюдження виборчих листівок, розклеювання виборчих плакатів, публічні заклики голосувати за або проти кандидатів на пост Президента України;
- закінчення розповсюдження політичної реклами;
- зняття передвиборних агітаційних матеріалів з 24.00 останньої п'ятниці, що передує дню виборів чи дню повторного голосування, відповідними службами місцевих органів виконавчої влади та органів місцевого самоврядування;

3) заборонено оприлюднення в день виборів результатів опитування виборців щодо їх волевиявлення (так звані exit-polls) під час голосування до його закінчення, тобто до 20.00 дня виборів.

Згідно з національним законодавством, будь-яка особа може подати заяву про відомі їй порушення виборчого законодавства до Центральної виборчої комісії, територіальних виборчих комісій або безпосередньо до правоохоронних органів (міліції, прокуратури, Служби безпеки України) чи суду загальної юрисдикції (місцевого, апеляційного).

Передбачено обов'язок Центральної виборчої комісії (ЦВК) або територіальної виборчої комісії у разі надходження до неї заяви або скарги про порушення, які мають ознаки адміністративного або кримінального правопорушення, негайно надіслати цю заяву або скаргу до відповідних правоохоронних органів для перевірки і реагування згідно із законами України.

Інформаційні правовідносини виникають також із приводу передачі результатів народного волевиявлення до тервиборчкомів та ЦВК. Ця інформація передається на паперових носіях у вигляді протоколів з мокрими печатками, попередня інформація про результати голосування – телеграфним зв'язком та в електронному вигляді у формі електронних протоколів.

Механізмом захисту інформації про результати народного волевиявлення передбачене право членів виборчих комісій, спостерігачів, довірених осіб та самих кандидатів отримувати копії протоколів виборчих комісій з підсумками голосування, завірених головою та секретарем комісії і скріплених печаткою.

Правила використання ЦВК автоматизованої інформаційної системи при проведенні виборів народних депутатів України, Президента України, всеукраїнського референдуму визначаються ст. 25 Закону України “Про Центральну виборчу комісію”¹²⁷. Згідно з її нормами, під час процедури голосування автоматизована інформаційна система використовується виключно для спостереження за ходом і результатами голосування. Відомості про результати голосування, отримані через автоматизовану інформаційну систему, є попередньою інформацією, що не має юридичних наслідків.

Одним із заходів забезпечення достовірності інформації, що передається за допомогою цієї системи, є встановлене законодавством

¹²⁷ Про Центральну виборчу комісію: Закон України від 30 червня 2004 р. № 1932-IV // Відомості Верховної Ради України. – 2004. – № 36. – Ст. 448.

права членів ЦВК ознайомлюватися з будь-якою інформацією, що міститься в автоматизованій інформаційній системі Комісії або виводиться з неї.

Останнім часом сталися істотні зміни у правовому регулюванні виборів, зокрема, інформаційних відносин, що виникають у зв'язку з ними. Значно підвищилися роль та ефективність контролю з боку громадськості та інститутів громадянського суспільства.

4. 5. Захист персональних даних

Гарантії прав і свобод людини у сфері інформації однаковою мірою можуть стосуватись і реалізації прав, що дають змогу людині бути повноправним суб'єктом інформаційних відносин, і тих, що захищають людину від неправомірного інформаційного втручання. Але механізми і способи реалізації та захисту цих прав мають свою специфіку. Права першого типу, які забезпечують вільну участь в інформаційних відносинах, є практично самодостатніми, тобто для їх реалізації потрібне закріплення їх в нормативно-правових актах, воля суб'єкта та наявність механізмів, передусім судових, їх захисту. Захист від неправомірного інформаційного втручання, навпаки, вимагає передусім створення комплексу нормативно-правових актів, що регулюють діяльність органів державної влади, фізичних та юридичних осіб у сфері інформації з метою встановлення чітких юридичних рамок і параметрів такої діяльності. Крім того, проблемою захисту останнього типу прав є те, що, на відміну від порушень свободи слова, подібне втручання може мати прихований характер, але водночас створювати значну загрозу.

Крім конституційних норм статей 31 (таємниця листування) і 32 (невтручання в особисте життя) Конституції, в Україні діє низка правових актів, що конкретизують регулювання означених питань.

За допомогою окремих законодавчих актів, наприклад, конкретизується конституційний принцип невтручання в особисте життя. Закон України “Про інформацію”¹²⁸ (ст. 23) визначає інформацію про особу як сукупність документованих або публічно оголошених відомостей про особу, відносячи до них дані про: національність, освіту, сімейний стан, релігійність, стан здоров'я, а також

¹²⁸ Про інформацію: Закон України від 2 жовтня 1992 р. // Відомості Верховної Ради України – 1992. – № 48. – Ст. 650

адресу, дату і місце народження. Цією статтею встановлюються також основні принципи, що визначають режим доступу інформації про особу:

- забороняється збирання відомостей про особу без її попередньої згоди, за винятком випадків, передбачених законом;
- кожна особа має право на ознайомлення з інформацією, зібраною про неї;
- інформація про особу охороняється Законом.

Перелік відомостей, що не підлягають розголошенню, розширено також у ч. 3. ст. 46 Закону “Про інформацію”. Це відомості, що стосуються лікарської таємниці, грошових вкладів, прибутків від підприємницької діяльності, усиновлення (удочеріння), листування, телефонних розмов і телеграфних повідомлень.

Закон України “Про державну статистику” (ч. 1 ст. 21) до конфіденційної інформації відносить також: “первинні дані, отримані органами державної статистики від респондентів під час проведення статистичних спостережень, а також адміністративні дані щодо респондентів, отримані органами державної статистики від органів, що займаються діяльністю, пов’язаною із збиранням та використанням адміністративних даних”¹²⁹.

Важливим елементом механізму забезпечення права людини на конфіденційність приватного життя можна розглядати встановлене ст. 31 Закону “Про інформацію” право громадян на доступ до інформації про них, зібраної органами державної влади та місцевого самоврядування. Це право (ч. 1. ст. 31) визначає право громадян знати у період збирання інформації, які відомості про них і з якою метою збираються, як, ким і з якою метою вони використовуються та право громадян мати доступ до інформації про них, і в разі потреби, заперечувати її правильність, повноту, доречність тощо.

Через звернення до органів державної влади та місцевого самоврядування громадянин може встановити сам факт збирання відомостей про нього, їх зміст і мету збирання, а тому і ставити питання про законність відповідних дій. Органи публічної влади зобов’язані надавати подібну інформацію безперешкодно і безкоштовно на вимогу осіб, яких вона стосується, крім випадків, передбачених законом (коли подібна інформація є державною або службовою таємни-

¹²⁹ Про державну статистику від 17 вересня 1992 р. // Відомості Верховної Ради. – 1992. – № 43. – Ст. 608 (В редакції Закону № 1922-III від 13. 07. 2000 / ВВР, 2000. - № 43. – Ст. 362)

цею), а також вживати заходів щодо запобігання несанкціонованому доступу до неї. Передбачено право громадян (ч. 7 ст. 31 Закону “Про інформацію”) оскаржувати в суді відмову в доступі до такої інформації або приховування її чи незаконні збирання, використання, зберігання чи поширення. Крім того, відповідно до ст. 56 Конституції та ч. 2 ст. 31 Закону “Про інформацію”, гарантується право на захист та відшкодування за рахунок держави матеріальної і моральної шкоди, заподіяної незаконними діями органів публічної влади щодо інформації про особу.

Як зазначалося, в більшості випадків збирання персональних даних здійснюють органи державної влади та місцевого самоврядування. Таким чином, багато в чому питання реальності, а не декларативності комплексу прав, що охороняють недоторканність особистого життя, стосується сфери організації діяльності органів публічної влади. В межах соціального управління, яке здійснюють відповідні органи державної влади та місцевого самоврядування, формуються конкретні механізми забезпечення гарантованих Конституцією умов участі людини в інформаційних процесах. Керуючись духом і змістом правової та адміністративної реформ, які здійснюються в Україні, можна говорити про те, що “створення дійових механізмів забезпечення прав і свобод людини є одним з орієнтирів трансформації адміністративного права”, одним з напрямів досягнення цієї мети можна назвати “деталізацію закріплених у Конституції України процедур, не пов’язаних з юрисдикційною діяльністю органів виконавчої влади і суду”¹³⁰.

Такими процедурами є, зокрема, процедури захисту конфіденційної інформації про особу в органах державної влади, процедури захисту інформації в комунікаційних системах, що забезпечує таємницю кореспонденції тощо.

Однією з ключових проблем дотримання прав і свобод людини у сфері захисту персональних даних є можливі порушення процесів правоохоронної діяльності держави. Ця діяльність усе ще потребує значного реформування, аби відповідати вимогам демократичного суспільства. Самі працівники органів внутрішніх справ, визнаючи ступінь розповсюдженості різних видів службових порушень, зокрема, називають такі: невинуватене насильство; порушення прав

¹³⁰ Скриль С. А. Адміністративно-правові засоби реалізації прав людини в Україні // Актуальні проблеми політики: 36. наук. праць. – Вип. 13 – 14. – Одеса, 2001. – С. 194.

громадян (58,3% респондентів); ухилення від допомоги громадянам (46,2%); хабарництво, корупція, вимагання (44,8%)¹³¹.

Окреслюючи шляхи забезпечення інформаційних прав людини в цій сфері, основну увагу слід акцентувати на забезпеченні суворого виконання норми ч. 2. ст. 6 Конституції України, яка визначає, що владні інституції “здійснюють свої повноваження у встановлених Конституцією межах і відповідно до законів України”¹³². Це, здавалося б, просте завдання залишається дуже актуальним в українських реаліях. Особливо, якщо враховувати давню традицію прийняття підзаконних нормативно-правових актів, здатних перекручувати, зменшувати або розширювати тлумачення змісту законів та низькій рівень правосвідомості.

Зазначимо, що Україною від самого проголошення незалежності обрала курс на перебудову своєї правоохоронної системи у бік демократизації та поваги до прав людини. На жаль, це стосується більшою мірою законотворчості, ніж правозастосування.

Так уже в 1990 р. в Законі “Про міліцію”¹³³ було викладено основні принципи регламентування відносин між органами внутрішніх справ (ОВС) і громадянами. Заслугує на увагу ст. 5 цього Закону, присвячена співвідношенню діяльності ОВС та додержанню прав громадян.

Серед важливих гарантій додержання прав людини можна назвати принцип установлення компетенції ОВС виключно законом. Відповідно до ч. 1 ст. 5 Закону “Про міліцію”, вона виконує свої завдання неупереджено, у точній відповідності із законом. Її обов’язки і повноваження перелічені в ст. 10 і 11 цього Закону. До того ж, наступною нормою підкреслюється вичерпність наданих міліції прав, те, що ніякі виняткові обставини чи вказівки службових осіб не можуть бути підставою для будь-яких незаконних дій або бездіяльності міліції.

Серед інших принципів, передбачених ст. 5 Закону “Про міліцію”, що визначають взаємини ОВС і впливають на рівень захищеності прав міліції у сфері інформації, зазначено:

¹³¹ Бандурка О. М., Соболєв В. О. Теорія та методи роботи з персоналом в органах внутрішніх справ. – Х.: Вид-во Ун-ту внутр. справ, 2000. – С. 266 – 267.

¹³² Конституція України. Прийнята Верховною Радою України 28 червня 1996 р. // Відомості Верховної Ради. – 1996. – № 30. – Ст. 141.

¹³³ Про міліцію: Закон України від 20 грудня 1990 р. № 565-XII // Відомості Верховної Ради. – 1991. – № 4. – Ст. 20.

- обов'язок працівника міліції при звертанні до громадянина назвати своє прізвище, звання та пред'явити на його вимогу службове посвідчення;
- заборона ОВС розголошувати відомості, що стосуються особистого життя людини, принижують її честь і гідність, якщо виконання обов'язків не вимагає іншого;
- обов'язок ОВС дати громадянам пояснення з приводу тимчасового обмеження прав і свобод громадян, яке може бути здійснено лише в межах чинного законодавства, і лише якщо без цього не можуть бути виконані покладені на неї обов'язки;
- обов'язок ОВС не пізніше як через 24 години повідомити про місцеперебування затриманих і взятих під варту осіб близьким родичам, адміністрації за місцем роботи чи навчання.

Отже, законодавчі приписи створюють доволі міцну правову базу гарантування прав і свобод людини в процесі виконання ОВС своїх повноважень. Інша річ, що практика досить часто свідчить про невиконання або неналежне виконання міліцією відповідних правових норм. Але це проблема не тільки правової, а й інституціональної реформи.

Механізм і умови обмеження інформаційних прав і свобод людини визначаються низкою законодавчих актів, що регулюють питання правоохоронної діяльності та компетенцію правоохоронних органів, зокрема Кримінально-процесуальний кодекс України, Закони України “Про оперативно-розшукову діяльність”, “Про прокуратуру”, “Про Службу безпеки України”, “Про прикордонні війська”, “Про державну податкову службу в Україні” та ін.

Наприклад, нормами ст. 4. Закону “Про оперативно-розшукову діяльність” передбачено, що ця діяльність “ґрунтується на принципах законності, дотримання прав і свобод людини, взаємодії з органами управління і населенням”¹³⁴. Наступні норми цього Закону деталізують і визначають механізми дотримання зазначених принципів. Зокрема, комплекс гарантій законності та дотримання прав і свобод людини під час здійснення оперативно-розшукової діяльності визначено ст. 9 цього Закону:

- ч. 5 ст. 9 Закону про ОРД визначено, що під час здійснення оперативно-розшукової діяльності не допускається порушен-

¹³⁴ Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135-XII. // Відомості Верховної Ради. – 1992. – № 22. – ст. 303.

ня прав і свобод людини та юридичних осіб. (Окремі обмеження цих прав і свобод мають винятковий і тимчасовий характер і можуть застосовуватись лише за рішенням суду щодо особи, в діях якої є ознаки тяжкого злочину, та у випадках, передбачених законодавством України, з метою захисту прав і свобод інших осіб, безпеки суспільства);

- встановлено відповідальність правоохоронних органів у разі порушення прав і свобод людини або юридичних осіб у процесі здійснення оперативно-розшукової діяльності, а також їх обов'язок невідкладно поновити порушені права і відшкодувати заподіяні матеріальні та моральні збитки, в т. ч. і в разі не підтвердження причетності до правопорушення особи, щодо якої здійснювались оперативно-розшукові заходи. (ч. 8 ст. 9).

Низка норм цієї статті гарантує безпосередньо інформаційні права та інформаційну безпеку людини, серед цих:

- право особи у встановленому законом порядку одержати від органів, на які покладено здійснення оперативно-розшукової діяльності, письмове пояснення з приводу обмеження її прав і свобод та оскаржити ці дії;
- заборона зберігати або розголошувати одержані внаслідок оперативно-розшукової діяльності відомості, що стосуються особистого життя, честі, гідності людини, якщо вони не містять інформації про вчинення заборонених законом дій або порушення прав людини (такі відомості підлягають знищенню);
- заборона застосовувати для одержання інформації технічні засоби, психотропні, хімічні та інші речовини, які пригнічують волю або завдають шкоди здоров'ю людей та навколишньому середовищу.

Доступ громадян до інформації про них, яка збирається у зв'язку з їх зверненнями до ОВС, визначається нормами Положення про порядок роботи зі зверненнями громадян і організації їх особистого прийому в системі Міністерства внутрішніх справ України (п. 9)¹³⁵. Згідно з цим Положенням у період збирання інформації, необхідної для здійснення перевірки за зверненнями, громадяни мають право:

- знати, які відомості про них, з якою метою збираються, як, ким і з якою метою вони мають використовуватися.

¹³⁵ Про затвердження Положення про порядок роботи зі зверненнями громадян і організації їх особистого прийому в системі Міністерства внутрішніх справ України: Наказ МВС України від 10 жовтня 2004 р. № 1177.

- доступу до інформації про них, заперечувати її правильність, повноту, об'єктивність тощо.

Крім того, встановлюються правила збирання, зберігання та використання такої інформації, спрямовані на забезпечення конфіденційності персональних даних. Ці правила передбачають:

- недопущення доступу сторонніх осіб до відомостей про іншу особу, зібраних відповідно до законодавства;
- обмеження терміну зберігання інформації про громадян, який не повинен тривати довше встановленого строку зберігання матеріалів перевірки за зверненнями;
- кількість даних про громадян, отримана під час перевірки звернення, має бути максимально обмеженою і може використовуватися лише з метою перевірки викладених у зверненні відомостей.

Певний комплекс норм, спрямованих на забезпечення захисту персональних даних і таємниці кореспонденції, міститься в законодавстві України, що регулює питання телекомунікацій і поштового зв'язку. Так, ст. 9 Закону України “Про телекомунікації” встановлює обов'язок операторів і провайдерів телекомунікацій вживати відповідно до законодавства технічних та організаційних заходів щодо захисту телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж та інформації, що передається цими мережами.

Нормами ст. 34 Закону України “Про телекомунікації” визначаються обов'язки операторів і провайдерів телекомунікацій щодо захисту інформації про споживача. Цей захист має кілька аспектів, зокрема:

- обов'язок операторів та провайдерів телекомунікацій забезпечувати схоронність відомостей про споживача, отримані при укладенні договору, надані телекомунікаційні послуги, у т. ч. про отримання послуг, їх тривалість, зміст, маршрути передавання тощо;
- обов'язок операторів телекомунікацій під час автоматизованої обробки інформації про абонентів забезпечувати її захист відповідно до закону;
- можливість включення у призначені для оприлюднення телефонні довідники, у т. ч. електронні версії та бази даних інформаційно-довідкових служб інформації про прізвище, ім'я,

по батькові, найменування, адресу та номер телефону абонента *лише в разі*, якщо в договорі про надання телекомунікаційних послуг зазначено про згоду споживача на опублікування такої інформації;

- право споживача на безоплатне вилучення відомостей про нього повністю або частково з електронних версій баз даних інформаційно-довідкових служб.

Обов'язок операторів поштового зв'язку вживати організаційно-технічних заходів щодо захисту інформації, згідно із законодавством щодо захисту таємниці кореспонденції встановлено ст. 6 Закону України “Про поштовий зв'язок”.

Виймка та огляд письмової кореспонденції, вкладень в інших поштових відправленнях, одержання будь-яких довідок щодо них заборонено, крім випадків, визначених законом.

Заборонені до пересилання вкладення у поштових відправленнях вилучаються операторами із поштового відправлення у встановленому відповідно до цього Закону порядку в присутності відправника або уповноваженої ним особи, крім випадків, установлених законом.

Єдина процедура обмеження права людини на таємницю кореспонденції визначається ст. 187 Кримінально-процесуального кодексу України¹³⁶. Ця процедура передбачає накладення арешту на кореспонденцію або зняття інформації з каналів зв'язку лише за постановою апеляційного суду, причому в цій постанові вказується особа, види кореспонденції або канал зв'язку і термін здійснення таких дій.

На тлі подібних законодавчих гарантій не зовсім логічною виглядає норма ч. 4 ст. 39 Закону України “Про телекомунікації”, за якою оператори телекомунікацій зобов'язані власним кошти установлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових заходів та не допускати розголошення організаційних і тактичних прийомів їх проведення.

Фактично ця норма передбачає, що споживачі телекомунікаційних послуг, за рахунок плати яких і формуються кошти операторів, повинні самі оплачувати встановлення обладнання для зняття інформації з каналів зв'язку, тобто для обмеження їх прав на таємницю ко-

¹³⁶ Кримінально-процесуальний кодекс України. – К., 2001.

респонденції. В цьому контексті позитивним можна вважати лише обов'язок операторів телекомунікацій забезпечувати захист зазначених технічних засобів від несанкціонованого доступу.

Загалом досить поширеними є думки щодо необхідності вдосконалення законодавства, що забезпечує механізми захисту особистих даних, особливо в межах діяльності органів виконавчої влади щодо інформації, яку вони збирають відповідно до своєї компетенції.

ГЛАВА 5. ІНФОРМАЦІЙНА БЕЗПЕКА

Історія формування категорій “національна безпека” і “національні інтереси”. Поняття і правові основи інформаційної безпеки України. Напрями державної політики у сфері інформаційної безпеки. Інституціональний механізм інформаційної безпеки. Міжнародно-правові основи інформаційної безпеки.

5. 1. Історія формування категорій “національна безпека” та “національні інтереси”.

Інформаційна безпека останнім часом стала одним із найважливіших напрямів інформаційної діяльності. Важливість цього напрямку зумовлена низкою чинників. Передусім це ключова організаційно-управлінська та регулятивно-контрольна функція інформаційного чинника в сучасному суспільстві. Але пропорційно до збільшення ролі цього чинника зростають і можливі суспільно-небезпечні наслідки від протиправного втручання в інформаційні відносини і процеси. Крім того, в умовах сучасних глобалізаційних тенденцій Україна має бути спроможною адекватно відповідати на всі виклики та небезпеки, пов'язані з розбудовою глобального інформаційного суспільства.

У загальному вигляді інформаційна безпека виступає складовою або підсистемою такої категорії, як “національна безпека”¹³⁷. Це поняття має велику кількість вимірів та аспектів, різниця між якими зумовлена і за відповідними позиціями, з яких розглядається це питання. Навіть за наявності певних принципових узгоджень щодо методології та системи світогляду відразу помітні розбіжності в баченні сутності та змісту національної безпеки у фахівців-правників на відміну від військових, економістів, політологів та ін. Оскільки метою цього розділу є аналіз різних аспектів інформаційної складової національної безпеки саме з позицій юридичної науки, причому під адміністративно-управлінським кутом зору, то і підхід до цієї

¹³⁷ Див. докл.: *Кормич Б. А.* Інформаційна безпека: організаційно-правові основи: Навч. Посібник. – К. : Кондор, 2004. – С. 16–39.

проблеми буде певною мірою обмежений наявними організаційно-правовими засадами.

Навіть у межах окресленого організаційно-правового підходу можна виділити дві самостійні сфери існування понять національної безпеки та її інформаційного компонента. По-перше, це теоретична сфера національної безпеки, яка розглядає окреслену проблему щодо розуміння її змісту й сутності, визначення її місця в системі державної діяльності тощо.

По-друге, це практична сфера національної безпеки, що розглядає нормативно-правові основи діяльності держави, спрямовані на захист національної безпеки та на створення відповідних дієвих механізмів цього захисту.

Категорія “національна безпека” виникла як зовнішньополітична і є цілком американським винаходом. Вперше на державному рівні це поняття було використано в 1904 р. в посланні тодішнього президента США Теодора Рузвельта конгресу США, в якому він обґрунтовував приєднання зони Панамського каналу інтересами національної безпеки¹³⁸.

Відтоді національна безпека стала об’єктом досліджень у сфері спочатку політичної науки, а згодом, коли цей термін із політичного лексикону перейшов у нормативно-правові акти, – і юридичної науки. Ще одним певною мірою відокремленим напрямом розроблення проблем національної безпеки можна вважати так звані “стратегічні дослідження”, тобто відповідний аналіз зовнішньо- та внутрішньополітичної ситуації з урахуванням широкого спектра об’єктивних суб’єктивних чинників, які здійснюють спеціальні установи на замовлення центральних органів державної влади і результати якого використовуються, останніми для прийняття політичних рішень.

Щодо “чистої” американської концепції національної безпеки значимо, що вона ґрунтується на теорії “національних інтересів”, і саме звідси бере початок відповідна модель співвідношення, в якій національна безпека розглядається як частина національних інтересів. Така модель нині набула широкого визнання. Вперше її запропонував американець У. Липпман. Дослідниками цієї проблеми були також Б. Броуді, М. Гальперін, Г. Кан, Г. Кіссінджер, Г. Ласвел, Г. Моргентау, Дж. Шлессінджер.

¹³⁸ Политология: энциклопедический словарь / Общ. ред. и сост. Ю. И. Аверьянов. – М. : Изд-во Моск. коммерч. ун-та., 1993. – С. 197 – 198.

Однією із особливостей американської школи слід назвати розроблення двох принципових підходів, один із яких пов'язує національну безпеку з могутністю держави, що і створює *ресурс* захисту безпеки, а другий ставить на перше місце міжнародну співпрацю як створення *умов* гарантування національної безпеки.

Розглядаючи історію введення в політичний і правовий обіг категорій “національна безпека” та “національні інтереси”, зазначимо певний негативний аспект їх застосування. Від початку ці поняття стали використовувати для обґрунтування принципово протиправних і антидемократичних дій. Тобто йдеться про певні неузгодженості правотворчого і правозастосовного аспектів цих категорій. Вони несуть певний відбиток харизматичності, перетворилися на зручний інструмент спочатку міжнародної, а згодом і внутрішньої політики. Виникнення їх саме в міжнародній сфері також має своє пояснення. На початку ХХ ст. міжнародне право вже склалося в чітку систему, яка значною мірою обмежувала дії держав, і, отже, потрібно було знайти виправдання порушенню цих обмежень. А обґрунтування зневаги до норм міжнародного права необхідністю захисту національної безпеки виявилось цілком дієздатним. На жаль, така сама доля спіткала й застосування категорії національної безпеки у внутрішній сфері, яка, також, почали використовувати в США як привід для обмеження громадянських свобод. Прикладом став *Communist Control Act*, або Закон про контроль за комуністами 1950 р., згідно з яким кожна організація, визнана комуністичною, відразу оголошувалася незаконною і втрачала будь-які права.

В СРСР подібна термінологія не використовувалася, а перші розробки в цій сфері з'явилися в 1990 р. зі створенням Фонду національної та міжнародної безпеки. Можливо, це можна пояснити тим, що СРСР мав власні, що ґрунтувалися на комуністичній ідеології, методи пояснення своїх, часто протиправних, дій.

Процес захисту державою своїх інтересів та безпеки безпосередньо пов'язаний із проведенням державної політики, в межах якої і здійснюються конкретні заходи їх реалізації. Зокрема, існує думка про те, що “національна безпека – це державна політика, скерована на створення внутрішніх і міжнародних умов, сприятливих для збереження чи зміцнення життєво важливих національних цінностей; це стан, що забезпечує захищеність інтересів народу й держави, суспільства та кожного його члена”¹³⁹.

¹³⁹ Політологія / За ред. О. В. Бабкіної, В. П. Горбатенка. – К.: Академія, 1998. – С. 316.

Проте будь-якій інтерпретації поняття “безпека” та “небезпека” пов’язані з умовами існування певного об’єкта, що характеризується, відповідно, відсутністю або наявністю реальної чи потенційної загрози. А політика, яка є певною системою заходів відповідної спрямованості, виступає як інструмент, що змінює або намагається змінити в той чи інший бік умови існування об’єкта, повертаючи вектори розвитку в бік зменшення чи збільшення загрози.

Складовими сучасної системи безпеки є такі:

- доктрина і правова основа, якими визначаються основні завдання і принципи державної діяльності щодо захисту безпеки;
- інституціональний механізм, тобто сукупність міжнародних і національних державних і громадських органів, які в своїй діяльності вирішують певні завдання щодо підтримання стану безпеки різних рівнів;
- методологічна база, тобто способи, засоби й ресурси, що використовуються для реалізації конкретних завдань у межах політики безпеки.

Безпосередній зв’язок поняття “безпека” з конкретним об’єктом та його умовами існування робить цей об’єкт головним критерієм класифікації видів безпеки.

За об’єктним складом (особа, суспільство або держава, що є об’єктом загрози) розрізняють безпеку: міжнародну (безпеку багатьох держав), окремої держави, особисту (безпеку конкретної особи) та суспільну (безпеку невизначеного кола осіб). За сферою суспільних відносин, що є об’єктом загрози, виокремлюють безпеку: інформаційну, військову, економічну, політичну, екологічну, санітарно-епідеміологічну, культурну, технологічну, ядерну, пожежну, безпеку дорожнього, залізничного та повітряного руху, безпеку мореплавства та ін. Хоча буває досить важко розрізнити види безпеки, або безпеку одного суб’єкта та безпеку інших суб’єктів.

Загалом сучасні процеси глобалізації призводять до певного стирання меж між внутрішньодержавними і міжнародними проблемами. Будь-які критичні ситуації в одній державі (порушення прав людини, екологічна або економічна криза, соціальні, національні або військові конфлікти) миттєво позначаються на стабільності й розвитку цілих регіонів і можуть перетворитися на міжнародні.

Реалії сьогодення не оминули і таку досить консервативну сферу, як національна безпека. Причому йдеться не про загальні цілі, які є

певного роду догмою для будь-якої держави, а насамперед про засоби, якими досягають цих цілей.

Домінуючими в цій трансформації стали два чинники. По перше, внаслідок розподілу СРСР та закінчення “холодної війни” зникла або значно зменшилася загроза глобального військового конфлікту. По-друге, нинішній світ, принаймні його розвинена частина, охоплений процесами глобалізації та інтеграції. Все це зумовило певний зсув векторів у національних системах, зокрема включення в них елементів глобалізації. За деякими концепціями “національна безпека” певною мірою втрачає свій державний або блоковий характер, перетворюючись на глобальне явище, що частково залежить не від потужності держави, блоку чи угруповання держав, а від процесів міждержавної та міжнародної співпраці.

Подібними міркуваннями зумовлена і поява специфічного терміну “кооперативна безпека”. На думку Д. Дьюїта, основами цієї нової системи кооперативної безпеки стають три елементи:

- спрямованість не на залякування агресора, а на створення твердих гарантій запобігання агресії;
- альтернативність політиці союзів або принаймні співіснування поряд з ними;
- просування в галузі не лише військової, а й невійськової безпеки¹⁴⁰.

Характерними її рисами стає зменшення військових зовнішніх загроз на тлі розвитку низки процесів як глобального, так і регіонального характеру, що негативно впливають на внутрішню безпеку. Такими негативними процесами є: нові громадянські та міжнаціональні, міжконфесійні конфлікти, масові порушення прав людини, зростання насильства, розповсюдження наркотиків, тероризму, епідемії та екологічні проблеми. Саме просування векторів небезпеки від військових до невійськових і зумовлює потребу кожної держави приділяти увагу поліпшенню своєї внутрішньої безпеки.

Зі зсувом основних загроз у невійськову площину безпосередньо пов’язане деяке протиставлення індивідуальної безпеки та безпеки держави. Цікавою щодо цього думка колишнього міністра закордонних справ Канади Ллойда Ексвордсі, який вважає, що, попри посилення міжнародної безпеки, безпека людей стає менш гарантованою через зростаючу кількість внутрішніх конфліктів. Він вважає, що саме

¹⁴⁰ Dewitt D. Common, Comprehensive and Cooperative Security. – The Pacific Review, 1994. – V.

ці внутрішні конфлікти та зазначені вище негативні чинники, з якими держава або не може, або не бажає боротися, спростовують гіпотезу, що безпека особи залежить від безпеки держави. Л. Ексвордсі пов'язує зміцнення безпеки, особливо безпеки людини, в сучасному світі із впровадженням принципово нової наднаціональної стратегії кооперативної безпеки, яка має шість складових, саме:

- система індивідуальної безпеки потребує енергійного втручання для захисту людського життя, зокрема, застосування примусових заходів серед яких санкції та військове втручання;
- важливо оцінити людські “витрати” стратегій безпеки – як міжнародних, так і пов'язаних із безпекою окремої держави;
- політика безпеки має бути тісно інтегрована у стратегію підтримання прав особистості, демократії та розвитку;
- зважаючи на складний характер сучасних викликів безпеці індивідів, ініціативи в цій сфері мають бути спрямовані до суб'єктів світової спільноти, включаючи держави, багатосторонні організації та групи громадянського суспільства, а оскільки проблеми безпеки особистості мають транснаціональну природу, лише багатостороння співпраця дасть знайти ефективні рішення;
- результативність цих рішень залежатиме від посилення операційної координації, тобто чітко погоджених дій різних суб'єктів, зокрема учасників політичних переговорів, “блакитні шоломи”, спостерігачів за правами особи та відповідальних за гуманітарну допомогу;
- зростаючу роль у концепції безпеки відіграють неурядові організації – органи громадянського суспільства, які в багатьох випадках були у найбільш ефективними партнерами в зусиллях щодо захисту безпеки людей¹⁴¹.

Загалом політика національної безпеки держави спрямована на зменшення й уникнення наявних та можливих загроз нормальному розвитку держави відповідно до її цілей і є частиною національних інтересів країни.

Характеризуючи поняття національних інтересів, потрібно усвідомлювати, що інтерес взагалі – це “об'єктивно зумовлений мотив діяльності окремої людини, соціальної спільноти, суспільства в цілому,

¹⁴¹ *Axworthy L.* La securite humaine: la securite des individus dans un monde en monde. – Politique étrangere. – 1999. – N. 2. – P. 333.

спрямований на досягнення мети”¹⁴². Він має таку структуру: конкретні об’єктивні умови існування суб’єкта цього інтересу, суб’єктивна система цінностей, яка зумовлює конкретні завдання та необхідність їх досягнення і, нарешті, конкретна мета (завдання), що стоїть перед суб’єктом. Отже, якщо поняття національної безпеки виражає стан захищеності держави, її громадян від різних загроз, то поняття національних інтересів – зміст головних цінностей, цілей і прагнень суспільства й держави на конкретно-історичному етапі розвитку. Національні інтереси – це “інтегральний вираз інтересів усіх членів суспільства, що реалізуються через політичну систему відповідної держави, як компроміс у поєднанні запитів кожної людини і суспільства в цілому”¹⁴³.

Державна політика завжди виражає і представляє певний суспільний інтерес¹⁴⁴. У формуванні державної політики виражаються інтереси держави та суспільства загалом (національні інтереси) та інтереси окремих фізичних і юридичних осіб.

Категорія національних інтересів має системний характер у розумінні, що, з одного боку, вона є основою для визначення цілей і напрямів державної політики та діяльності органів публічної влади і політичної системи в цілому, а, з другого в – тому, що зміст національних інтересів формується у процесі розвитку держави й суспільства під впливом зовнішніх і внутрішніх об’єктивних чинників; у формуванні змісту національних інтересів беруть участь усі інститути держави, суспільства, окремі громадяни. Подібна ситуація потребує комплексного підходу до формування національних інтересів і характеризує його як досить складний процес, оскільки при визначенні єдиної загальнонаціональної системи потреб (інтересів) варто враховувати інтереси і потреби різних за характером суб’єктів (держави, її органів та інститутів, суспільства, суспільних груп, індивідів). Незрідка подібні інтереси можуть бути радикально протилежними і вступати в конфлікт. Для уникнення таких конфліктів і потрібні базові національні та державні цінності, які зазвичай формалізуються в нормах основних законодавчих актів держави.

¹⁴² Гелей С. Рутар С. Політологія. – К.: Знання, 1999. – С. 13

¹⁴³ Політологія / За редакцією О. В. Бабкіної, В. П. Горбатенка. – К.: Академія, 1998. – С. 322

¹⁴⁴ Кормич Б. А. Національна безпека як категорія аналізу законодавчого забезпечення державної політики / Парламентаризм в Україні: теорія і практика. Матеріали міжнар. науково-практ. конф., присвяченої 10-й річниці з дня проголошення Незалежності та 5-й річниці з дня прийняття Конституції України 26 червня 2001 р. – К., 2001. – С. 229.

Національна безпека співвідноситься з національними інтересами як частина й ціле і є важливою складовою національного інтересу держави, поряд із внутрішньою стабільністю, економічною успішністю, моральним здоров'ям суспільства, сприятливим зовнішнім оточенням, позитивним міжнародним іміджем¹⁴⁵. Безпечні умови існування – це одна з базових потреб як окремого індивіда, так і суспільства цілому, а отже, держави як територіальної організації суспільства.

Місце і роль такого чинника як безпека в житті особи та суспільства, те його вплива на легітимність державної влади добро пояснює ієрархічна теорія потреб американського психолога А. Маслоу. У межах цієї теорії виділено два типи потреб – базисні (постійні) та похідні (ціль потреби). Базисні потреби мають чітку ієрархію від нижчих до вищих, що складається із п'яти рівнів: фізіологічний, безпека, любов, самоствердження та самоактуалізація (творчість). Похідні (ціль-потреби) є рівнозначними, наприклад, потребам у справедливості, добробуті, порядку тощо.

Отже, на потребі в безпеці ґрунтується система потреб людини. Задоволення цієї потреби є основою подальшого розвитку й задоволення потреб більш високого рівня. Так само і в життєдіяльності держави за певних умов (наявність істотних зовнішніх або внутрішніх загроз) безпека може бути на першому плані, але у повсякденному бутті держави це лише один із багатьох напрямів її діяльності.

Як уже зазначалося, категорії національної безпеки та національних інтересів мають політичне походження і, набуваючи конкретного суспільного і державно-політичного змісту та значення, виражаються у нормах законодавства. Існує кілька сучасних концептуальних підходів до співвідношення функцій захисту національної безпеки та інших функцій держави.

Одним з найбільш широких є трактування питання національної безпеки законодавством Російської Федерації, з якого, до речі, Україна зробили низку запозичень.

Так, ч. 1 ст. 1 Закону Російської Федерації “Про безпеку” визначає що “Безпека – стан захищеності життєво важливих інтересів особи, суспільства та держави від внутрішніх та зовнішніх загроз”, а згідно з ч. 2 цієї статті, основними об'єктами безпеки є “особа – її права і свободи; суспільство – його матеріальні та духовні

¹⁴⁵ *Оборотов Ю. Н.* Современное государство: основы теории. – Одесса: Астропринт, 1998. – С. 64.

цінності; держава – її конституційний лад, суверенітет і територіальна цілісність”¹⁴⁶.

У цьому нормативно-правовому акті чітко простежується тенденція до створення всеохопної системи безпеки, адже така категорія, як інтереси особи, суспільства та держави, не має чітких меж, і будь-яка більш-менш значуща проблема може бути оголошена життєво важливим національним інтересом. Необхідність захисту подібного інтересу, в свою чергу, зумовлює узгоджену діяльність органів публічної влади для досягнення поставленого завдання. Так ч. 1 ст. 4 названого Закону встановлює, що: “Безпека досягається проведенням єдиної державної політики в галузі забезпечення безпеки системою заходів економічного, політичного, організаційного та іншого характеру, адекватних загрозам життєво важливим інтересам особи, суспільства та держави”. Фактично ця концепція забезпечує максимальне і практично необмежене втручання держави в усі практично всі аспекти життя людини і суспільства.

Дещо інший підхід до законодавчого визначення обсягів поняття “національна безпека” використано на батьківщині цього терміна – у США. Правовою основою забезпечення національної безпеки США є закон про національну безпеку 1947 р. – *The National Security Act of 1947*. На жаль, він безпосередньо не визначає терміна “національна безпека”. Але, згідно з указом президента США “Про класифіковану інформацію з національної безпеки” – *Classified National Security Information* (частина 1, секція 1. 1.), “національна безпека означає національну оборону або зовнішні відносини Сполучених Штатів”¹⁴⁷. Подібний підхід простежується практично в усіх нормативно-правових актах США з питань національної безпеки. Зовнішня спрямованість національної безпеки в її американському розумінні підкреслюється існуванням двох специфічних нормативно-правових актів – закону “Про національну безпеку” 1947 р. та закону “Про внутрішню безпеку” 1951 р. – *The internal security act of 1951*.

Відомі події 11 вересня 2001 р. справили величезний вплив на формування концепції національної безпеки в Сполучених Штатах і сприяли розширенню кола питань, які віднесено до цієї сфе-

¹⁴⁶ О безопасности: Закон Российской Федерации от 25 декабря 1992 г. № 4235-1 //Ведомости Верховного Совета РФ. – 1992. – №15. – Ст. 770.

¹⁴⁷ 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)

ри. Це виявилось і у виникненні нового терміна *homeland security*, який фактично є варіацією на тему внутрішньої безпеки і стосується насамперед запобігання терористичним атакам на території США. Цей термін запроваджено Законом “Про внутрішньодержавну безпеку” 2002 р. – *Homeland Security Act of 2002*, який трактує терміни *American homeland* та *homeland* як Сполучені Штати або територія Сполучених Штатів. Проте навіть у цьому разі такі питання, як, наприклад, екологія та соціальна сфера, до питань національної безпеки не включаються, на відміну від російської та української концепцій.

Значимо також, що обидві ці концепції належать державам, які мають загальновизнаний статус “наддержав” з виключно широкими геополітичними інтересами. Хоча відомі приклади ще більш прагматичного й обмеженого підходу до питань національної безпеки. Наприклад, це стосується досвіду Канади, яку об’єднує з Україною такий чинник як близьке сусідство з наддержавою (в її випадку із США, в нашому – із Росією). Так, за законом “Про розвідувальну службу безпеки Канади” (*Canadian Security Intelligence Service Act*) 1984 р., “питаннями, що стосуються безпеки Канади, є:

a) шпигунство або саботаж, спрямовані проти Канади або такі, що є шкідливими для інтересів Канади, чи діяльність, спрямована на підтримку такого шпигунства або саботажу;

b) діяльність, що чиниться під зовнішнім впливом усередині або щодо Канади, яка є шкідливою для інтересів Канади, таємною або оманною або містить загрозу для будь-якої особи;

c) діяльність усередині або щодо Канади, спрямована на підтримку загрози чи використання актів серйозного насильства проти осіб або майна з метою досягнення політичних цілей усередині Канади або іноземної держави;

d) діяльність, спрямована на підлив за допомогою таємних протиправних дій чи така, що має намір призвести врешті до руйнації чи повалення шляхом насильства конституційно заснованої системи державного управління в Канаді, але не включає законні адвокатський захист, протест або незгоду, якщо це не здійснюється у поєднанні з діяльністю, віднесеною до частин від (a) до (d)¹⁴⁸.

Як бачимо, порівняно з уже зазначеними трактуваннями національної безпеки, в канадському варіанті коло її питань значно зву-

¹⁴⁸ Canadian Security Intelligence Service Act. Chapter C-23. – 1984, C. 21, Sch.

жене і охоплює лише питання, критично необхідні для забезпечення нормальних умов існування держави.

Проте, як широке, так і вузьке трактування терміна “національна безпека” має переваги і вади. За своєю суттю вибір між цими двома трактуваннями можна розглядати в контексті дискусії щодо кількості та обсягу функцій, які має виконувати держава, інакше кажучи – питання про межі втручання держави в життя суспільства. Крім того, важливими є не тільки формальні межі державного втручання в інтересах національної безпеки, а і його зміст і методи. Тобто важливо не те, що робиться для захисту національної безпеки, а як робиться. Причому обидві концепції є актуальними і адекватними для відповідної держави, але ці актуальність і адекватність зумовлені передусім відповідністю цих концепцій геополітичним, економічним та соціальним реаліям, основним цілям і завданням держав, яким вони належать. Тому, аналізуючи проблеми національної безпеки конкретної держави, слід дуже обережно підходити до використання зарубіжного досвіду з огляду на індивідуальний зміст і характер безпеки кожної держави. Маючи однакові функціональні завдання захисту власної безпеки, різні держави, залежно передусім від геополітичних реалій, ставлять перед собою принципово різні цілі та обирають різні способи й методи їх досягнення.

Слід також зважати на те, що політичне походження зумовило перетворення національних інтересів та національної безпеки на такі собі “гумові” категорії, якими можна пояснити будь-які дії держави, що саме і створює потенційну небезпеку. Така ситуація надає важливого значення розвитку правового регулювання сфери національної безпеки. Основним завданням права щодо цього є чітке визначення сфери застосування таких категорій як національні інтереси та національна безпека, та визначення дієвих і контрольованих механізмів їх захисту, аби, з одного боку, забезпечити демократичний розвиток держави та суспільства, а з другого, створити справді безпечні умови цього розвитку.

5. 2. Поняття і правові основи інформаційної безпеки України.

Уперше в законодавчій практиці України питанню національної безпеки було приділено увагу в Декларації про державний суверенітет України від 16 липня 1990 р.¹⁴⁹. Ця декларація містить у собі розділ VII “Екологічна безпека” та Розділ IX “Зовнішня і внутрішня безпека”.

Акт проголошення незалежності України від 24 серпня 1991 р.¹⁵⁰ також оперує такими поняттями, як безпека та інтереси українського народу.

Спеціального нормативно-правового акту питань національної безпеки Україні довелося чекати ще цілих сім років, протягом яких відбулися докорінні трансформаційні процеси практично в усіх сферах суспільного життя. Ним стала ухвалена Верховною Радою 16 січня 1997 р. Постанова “Про концепцію (основи державної політики) національної безпеки України”¹⁵¹, яку було розроблено вже на основі нової Конституції України.

Цим документом уперше в законодавчій практиці України дано визначення понять “національна безпека” та “національні інтереси”, а також окреслено основні сфери, завдання, напрями та механізми їх захисту. Характерною є сама назва цього документу – Концепція (основи державної політики) національної безпеки. Тобто від початку питання національної безпеки безпосередньо пов’язано з державною політикою, з певними політичними процесами, що відбуваються в державі.

Конституція України¹⁵² містить норми, які визначають основні принципи регулювання сфери інформаційної безпеки.

По-перше, це норма ч. 1. ст. 17 Конституції України, яка визначає статус відповідного напрямку державної діяльності, встановлюючи, що захист інформаційної безпеки є однією з найважливіших функцій держави, справою всього Українського народу.

¹⁴⁹ Декларація про державний суверенітет України від 16 липня 1990 р. Відомості Верховної Ради України. – 1990. – № 31. – Ст. 429.

¹⁵⁰ Про проголошення незалежності України: Постанова Верховної Ради України від 24 серпня 1991 р. // Там само. – 1991. – № 38. – Ст. 502.

¹⁵¹ Про концепцію (основи державної політики) національної безпеки України: Постанова Верховної Ради України від 16 січня 1997 р. № 3/97-ВР // Голос України. – 1997. – 4 лют. – С. 5.

¹⁵² Конституція України. Прийнята Верховною Радою України 28 червня 1996 року // Відомості Верховної Ради України. – 1996. – №30 – Ст. 141.

У такий спосіб захист інформаційної безпеки виступає як самостійна функція, що є видом діяльності держави в інформаційній сфері і полягає як у захисті інформації з обмеженим доступом та інформаційних норм і відносин, так і в захисті особи, суспільства, держави від інформації, обмеженої Конституцією і законами.

По-друге, це група конституційних норм, якими визначаються ключові права людини у сфері інформації, забезпечення яких гарантує її інформаційну безпеку. Такими є норми ст. 31 Конституції України, що гарантують таємницю кореспонденції; норми ст. 32 Конституції України, які забороняють втручання в особисте та сімейне життя, збирання конфіденційної інформації про особу, гарантують право на спростування недостовірної інформації та відшкодування збитків від поширення такої інформації; норми ст. 34 Конституції України, які гарантують право на свободу думки і слова, на вільне вираження своїх поглядів і переконань.

І по-третє, слід виділити вкрай важливу конституційну норму, якою визначаються основні принципи забезпечення балансу між інтересами держави та правами й інтересами людини і громадянина у сфері інформаційної безпеки. Означена норма міститься в ч. 3 ст. 34 Конституції і передбачає обмеження свободи інформації в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам; для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя тощо.

Проблема балансу між інформаційними свободами людини і необхідністю державного втручання в інформаційні відносини є ключовою для ефективного захисту інформаційної безпеки. Її вирішення полягає у створенні дієвих механізмів захисту громадянами своїх прав та механізмів контролю з боку інститутів громадянського суспільства. Тому в демократичному суспільстві державне регулювання інформаційної сфери можливо лише через встановлення правових норм, що не суперечать змістові прав людини і забезпечують оптимальну взаємодію державних і недержавних інституцій.

Тривалий час у вітчизняному законодавстві не було визначення інформаційної безпеки. Зокрема, в Законі “Про основи національної безпеки України”¹⁵³ вживається лише загальний термін “національна

¹⁵³ Про основи національної безпеки України: Закон України від 19 червня 2003 р. № 964 – IV // Офіційний вісник України. – № 29. – с. 38. – Ст. 1433.

безпеку” (ст. 1), яка визначена як “захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам”. А питання інформаційної безпеки розглядається в цьому Законі як певні аспекти національних інтересів та національної безпеки в інформаційній сфері.

Цим же Законом виділено три об’єкти національної та, відповідно, інформаційної безпеки (ст. 3), до яких належать:

- 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 недоторканість.

У законодавстві України визначено також багато аспектів інформаційної безпеки з питань інформатизації та розвитку інформаційного суспільства. Так, поняття інформаційної безпеки міститься в Законі України “Про Концепцію національної програми інформатизації”. Згідно п. 3 розділу VI Концепції, “Інформаційна безпека є невід’ємною частиною політичної, економічної, оборонної та інших складових національної безпеки”¹⁵⁴. Проте цей Закон дещо інакше, ніж Закон “Про основи національної безпеки України”, визначає класифікацію об’єктів інформаційної безпеки. Так, уже в п. 3 розділу VI визначається об’єктами інформаційної безпеки названо:

- інформаційні ресурси;
- канали інформаційного обміну і телекомунікації;
- механізми забезпечення функціонування телекомунікаційних систем і мереж;
- інші елементи інформаційної інфраструктури країни.

Закон “Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки”¹⁵⁵ (ст. 13) зазначено, що проблеми інформаційної безпеки набувають особливого значення за швидкого розвитку глобального інформаційного суспільства, широкого використання ІКТ в усіх сферах життя.

¹⁵⁴ Про Концепцію Національної програми інформатизації: Закон України від 4 лютого 1998 року № 75/98-ВР // Відомості Верховної Ради України. – 1998. – № 27– 28. – Ст. 182.

¹⁵⁵ Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 9 січня 2007 р. № 537-V // Там само. – 2007. – № 12. – Ст. 102.

Ця стаття Закону дає нове визначення інформаційної безпеки, яке є узгодженим із встановленою законодавством дефініцією національної безпеки. За цією нормою: *інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.*

У цій дефініції сутність інформаційної безпеки розкривається через визначення певних ключових елементів (об’єктів) цієї безпеки, щодо яких потрібно вжити заходів забезпечення безпеки з метою унеможливлення шкоди. Такими елементами є:

- якість інформації, котру використовують (забезпечення її повноти, вчасності та вірогідності);
- правила інформаційної діяльності (запобігання негативному інформаційному впливу та негативним наслідкам застосування інформаційних технологій)
- правові режими інформаційних ресурсів та доступу до інформації (забезпечення виконання визначених законодавством правил розповсюдження та використання інформації, а також її цілісності, конфіденційності та доступності інформації).

Як уже зазначалося, характерною ознакою українського законодавства в галузі безпеки є наявність значних запозичень із законодавства Російської Федерації. Це, зокрема, стосується концептуальних положень про формування системи напрямів державної діяльності для захисту інформаційної безпеки на основі класифікації можливих загроз національним інтересам в інформаційній сфері. Наприклад, багато норм Закону “Про основи національної безпеки України” та Концепції (основ державної політики) національної безпеки України, що передувала йому, запозичено із закону Російської Федерації “Про безпеку”¹⁵⁶.

Доцільність подібних запозичень може викликати сумніви. Адже в нинішній редакції Закон України “Про основи національної безпеки України” має переважно декларативний характер. Зокрема, він не визначає конкретних механізмів захисту національної безпеки, зали-

¹⁵⁶ О безопасности: Закон Российской Федерации от 25 декабря 1992 г. № 4235-1 // Ведомости Верховного Совета РФ. – 1992. - №15. – Ст. 770.

шаючи реалізацію цих завдань у сфері проведення державної політики загалом; по-друге, не створює чітких критеріїв оцінювання стану національної безпеки та ефективності діяльності з її захисту.

Недоцільним, зокрема, є формування системи напрямів державної діяльності із захисту інформаційної безпеки на основі класифікації можливих загроз національним інтересам в інформаційній сфері, як це зроблено у більшості національних нормативно-правових актів та концепцій із цих питань. Адже такі категорії як “інтереси” і “загрози”, є мінливими та суб’єктивними, ступінь їх захищеності важко оцінювати. А правове регулювання вимагає стабільності та наявності чітких критеріїв оцінювання відповідності закону, ефективності захисту тощо.

Крім того, побудова правового регулювання на основі емпіричної концепції “можливих загроз” створює ризик перетворення питань інформаційної безпеки на певну “гумову категорію”, яка може використовуватися не для реального захисту держави, суспільства та окремої людини, а для обґрунтування гаслами захисту цієї безпеки таких дій, як порушення законодавства з боку державних органів, утиски свободи слова і прав людини тощо.

Загалом же захисту інформаційної безпеки можна визначити як складну систему, що складається з комплексу векторів державної політики і зумовлена специфікою об’єктів інформаційної безпеки¹⁵⁷.

В інформаційній безпеці слід виділити три комплекси питань, які диференціюються відповідно до природи правових норм, що становлять їх нормативно-правову базу:

1) інформаційна безпека людини і суспільства, яка ґрунтується, передусім на нормах природного права і вимірюється ступенем свободи від втручання держави та інших осіб, можливостями самореалізації та самовизначення;

2) інформаційна безпека держави, що ґрунтується на позитивному праві і пов’язана із застосуванням обмежень, заборон, жорсткою регламентацією. Невід’ємним елементом її є сила державного примусу;

3) інформаційна безпека суб’єктів підприємницької діяльності, яка насамперед має бути визначена законодавством з питань захисту конкуренції, регулювання економіки тощо.

¹⁵⁷ Кормич Б. А. Суб’єктно-об’єктний склад інформаційної безпеки // Актуальні проблеми політики: Зб. наук. праць. – Одеса: Юрид. літ-ра, 2003. – Вип. 19. – С. 395 – 399.

Комплекс питань інформаційної безпеки людини й суспільства має такі вектори:

- забезпечення інформаційних прав і свобод людини і громадянина;
- захист людини від неправомірного інформаційного втручання;
- забезпечення національної, культурної і духовної ідентичності від неправомірного втручання;
- забезпечення дієздатних правових та організаційних механізмів захисту відповідних прав та ін.

Комплекс питань інформаційної безпеки держави охоплює такі вектори державної діяльності:

- захист та обмеження обігу інформації з метою безпеки;
- захист інформаційної інфраструктури держави;
- безпека розвитку інформаційної сфери держави;
- захист національного інформаційного ринку;
- запобігання інформаційному тероризму та інформаційній війні, використання інформаційної зброї;

Комплекс питань інформаційної безпеки суб'єктів підприємницької діяльності включає такі вектори:

- захист комерційної таємниці;
- забезпечення захисту комерційної інформації органами державної влади;
- державний контроль за засобами захисту власної інформаційної безпеки, які використовуються комерційними підприємствами;
- дотримання безпечних параметрів інформаційних послуг та їх продуктів.

Отже, державно-правовий механізм інформаційної безпеки є системою органів державної влади загальної і спеціальної компетенції, задіяних у процесі формування та реалізації політики інформаційної безпеки, внутрішні й зовнішні ролі та відносини якої регулюються системою правових норм і принципів.

У складі цього державно-правового механізму є три взаємопов'язаних елементи:

1) сукупність державних інституцій, задіяних у процесі формування й реалізації політики інформаційної безпеки, тобто *інституціональний механізм інформаційної безпеки*;

2) сукупність ролей і відносин, передусім правових, що виникають у процесі проведення політики інформаційної безпеки, та спе-

цифічні форми і методи діяльності суб'єктів політики інформаційної безпеки;

3) ієрархічна сукупність правових норм і принципів, що регулює зміст і процес проведення політики інформаційної безпеки, тобто *правова база політики інформаційної безпеки*.

Основні способи реалізації державної політики у сфері інформаційної безпеки такі:

- розроблення нормативно-правових актів, що регулюють відповідні суспільні відносини в інформаційній сфері, встановлюють правила поведінки та відповідальність суб'єктів інформаційних правовідносин;
- створення нових державних інституцій і розширення компетенції існуючих у вирішенні завдань підтримання інформаційної безпеки;
- застосування у процесі діяльності державних інституцій конкретних, установлених правовими нормами засобів і напрямів державного впливу на інформаційну сферу.

5. 3. Основні напрями державної політики інформаційної безпеки

Закон України “Про основи національної безпеки” (ч. 2 ст. 5) визначає, що “національна безпека України забезпечується шляхом проведення виваженої державної політики”¹⁵⁸. Отже, саме політика називається головним “інструментом” досягнення необхідних безпечних умов суспільного і державного життя. До того ж, акцент зроблено саме на державній політиці, тобто такій, що проводиться від імені держави її владними органами. І це не дивно, адже саме в арсеналі державних засобів проведення політики є всім відомий інструмент державного примусу, який здебільшого й асоціюється із такими термінами, як “захист”, “безпека” тощо.

Ця сама норма визначає, що державна політика щодо забезпечення національної безпеки проводиться “відповідно до прийнятих в установленому порядку доктрин, концепцій, стратегій і програм у політичній, економічній, соціальній, воєнній, екологічній, науково-технологічній, інформаційній та інших сферах”.

¹⁵⁸ Про основи національної безпеки України: Закон України від 19 червня 2003 р. № 964 – IV // Офіційний вісник України. – № 29. – с. 38. – Ст. 1433.

Серед таких програмних документів найважливішими є Стратегія національної безпеки України і Воєнна доктрина України, які є обов'язковими для виконання і основою для розроблення конкретних програм за складовими державної політики національної безпеки. Ці документи розробляються на основі Закону “Про основи національної безпеки України” і затверджуються Президентом України.

Безпосередньо ж вибір конкретних засобів і шляхів забезпечення національної безпеки України зумовлений необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам загроз національним інтересам.

Крім того, політику національної, відповідно, інформаційної безпеки потрібно проводити лише в тих формах і тими методами й засобами, які притаманні і прийнятні демократичній правовій державі, тобто ґрунтуються на принципах демократії і верховенства права.

Це підтверджується нормами ч. 1. ст. 5 зазначеного Закону, які виділяють основоположні такі принципи державної діяльності в цій сфері:

- пріоритет прав і свобод людини і громадянина;
- верховенство права;
- пріоритет договірних (мирних) засобів у розв'язанні конфліктів;
- своєчасність і адекватність заходів захисту національних інтересів реальним і потенційним загрозам;
- чітке розмежування повноважень та взаємодія органів державної влади у забезпеченні національної безпеки;
- демократичний цивільний контроль над воєнною організацією держави та іншими структурами в системі національної безпеки;
- використання в інтересах України міждержавних систем та механізмів міжнародної колективної безпеки.

Як уже зазначалося, офіційна українська концепція безпеки побудована на позиціях визначення можливих загроз національним інтересам та встановлення адекватних відповідних заходів. Базові положення щодо визначення таких загроз і заходів містяться безпосередньо в Законі України “Про основи національної безпеки”, на основі якого розробляються інші, більш деталізовані програмні документи щодо захисту окремих напрямків національної безпеки. Слід зазначити, що норми цього Закону мають переважно декларативний характер, проте можуть давати уявлення про конкретні сфери і напрями реалізації державної політики в цій сфері.

Закон “Про основи національної безпеки України” розрізняє дві ключові категорії, які зумовлюють зміст і спрямованість державної політики у сфері інформаційної безпеки:

1) *загрози національним інтересам і національній безпеці України в інформаційній сфері* (ст. 7), до яких належать:

- прояви обмеження свободи слова й 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;

2) *основні напрями державної політики з питань національної безпеки в інформаційній сфері* (ст. 8):

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

Розглядаючи напрями державної політики у сфері інформаційної безпеки, варто назвати ще один законодавчий акт, який хоч і не стосується загальних питань інформаційної політики держави, проте визнає перспективні завдання в галузі інформаційної безпеки. Це Закон “Про Основні засади розвитку інформаційного суспільства в Україні на 2007– 2015 роки”¹⁵⁹, норми якого дають найбільш повне визначення інформаційної безпеки.

У п. 13 цього Закону визначено основні шляхи вирішення проблеми інформаційної безпеки:

- створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;
- підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;
- вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп’ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;
- розгортання та розвиток Національної системи конфіденційного зв’язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Як уже зазначалося, Закон “Про основи національної безпеки України” передбачає розроблення декількох програмних документів, які мають визначати конкретні напрями проведення державної політики щодо безпеки у різних сферах. Одним із таких ключових документів у сфері інформаційної безпеки є затверджена Указом Президента України *Стратегія національної безпеки України*¹⁶⁰. Вона визначає принципи, пріоритетні цілі, завдання й механізми забезпечення життєво важливих інтересів особи, суспільства і держави від зовнішніх і внутрішніх загроз. Ця Стратегія є базою для розроблення конкретних програм, проектів і планів заходів за складовими держав-

¹⁵⁹ Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 9 січня 2007 р. № 537-V // Відомості Верховної Ради України. – 2007. – № 12. – Ст. 102

¹⁶⁰ Про Стратегію національної безпеки України: Указ Президента України від 12 лютого 2007 р. № 105/2007.

ної політики національної безпеки та механізмів їх реалізації і розрахована на період досягнення визначених нею цілей.

Головною метою Стратегія визначає забезпечення такого рівня національної безпеки, який би гарантував поступальний розвиток України, її конкурентоспроможність, забезпечення прав і свобод людини і громадянина, подальше зміцнення міжнародних позицій та авторитету Української держави в сучасному світі. Однією із складових цього завдання є і забезпечення інформаційної безпеки.

Окремо визначено, що державна політика національної безпеки України формується та реалізується за умов, коли в сучасному світі нівелюється різниця між внутрішніми і зовнішніми аспектами безпеки, зростає вага несилових (політичних, економічних, соціальних, енергетичних, екологічних, *інформаційних*) (виділено нами – Б. К.) складових її забезпечення.

Характеризуючи основні негативні чинники, що впливають на стан захищеності національних інтересів України в інформаційній сфері. Стратегія визначає (п. 2. 8), що:

- посилюється негативний зовнішній вплив на інформаційний простір України, що загрожує розмиванням суспільних цінностей і національної ідентичності;
- недостатніми залишаються обсяги вироблення конкурентоспроможного національного інформаційного продукту;
- наближається до критичного стан безпеки інформаційно-комп'ютерних систем в галузі державного управління, фінансової і банківської сфери, енергетики, транспорту, внутрішніх та міжнародних комунікацій тощо.

Серед стратегічних пріоритетів політики національної безпеки (п. 3) зазначено низку таких, що стосуються сфери інформаційної безпеки, а саме:

- активізація інноваційних процесів в інформаційно-комунікаційній галузі, яка є елементом формування інфраструктури економіки знань – основу майбутньої конкурентоспроможності України у глобалізованому світі;
- запобігання поширенню в засобах масової інформації проявів насильства, расової, етнічної та релігійної нетерпимості, моральної розбещеності тощо;
- забезпечення інформаційної безпеки при інтеграції до структур глобального інформаційного суспільства.

Механізм реалізації державної політики інформаційної безпеки, відповідно до положень Стратегії національної безпеки, має складатися з трьох елементів: системи управління інформаційною безпекою, ресурсного забезпечення інформаційної безпеки та механізмів державного і громадського контролю за реалізацією цієї Стратегії.

Визначено також конкретні заходи, яких потрібно вжити в межах удосконалення механізму захисту інформаційної безпеки, зокрема:

- розвиток правових засад інформаційної безпеки, у т. ч. шляхом розробки та прийняття Національної стратегії формування інформаційного суспільства;
- розробка та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у т. ч. згідно з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність;
- підвищення ефективності діяльності суб'єктів забезпечення національної безпеки з упереджувального отримання інформації для своєчасного виявлення існуючих і нових типів внутрішніх і зовнішніх загроз, розробка дієвих заходів щодо їх запобігання та нейтралізації;
- інформаційно-аналітична підтримка діяльності органів державної влади, насамперед в умовах кризових і надзвичайних ситуацій, в т. ч. особливого періоду;
- впровадження захищених інформаційно-телекомунікаційних мереж в органах державної влади;
- розвиток інформаційно-телекомунікаційної інфраструктури.

Основним програмим документом, що визначає напрями діяльності держави щодо захисту національної безпеки у військовій сфері та прийняття якого прямо передбачене законодавством, є *Воєнна доктрина України*¹⁶¹. Це сукупність керівних принципів, воєнно-політичних, воєнно-стратегічних, воєнно-економічних та військово-технічних поглядів на забезпечення воєнної безпеки держави. У ній значну увагу приділено і питанням інформаційної безпеки та інформаційного забезпечення оборонної діяльності. Так, згідно з п. 1 Воєнної доктрини зазначено що воєнно-політична обстановка навколо України характеризується динамічністю й нестабільністю подій і процесів, які виникають внаслідок низки чинників, одним із яких є поява

¹⁶¹ Про Воєнну доктрину України: Указ Президента України від 15 червня 2004 р. № 648/2004.

новітніх видів і систем зброї, інформаційних технологій, що змінюють традиційні уявлення про характер збройної боротьби.

Зростанням ролі інформаційних технологій зумовлені такі ознаки сучасної збройної боротьби:

- широке застосування новітніх систем озброєння та військової техніки, зокрема, розвідки та радіоелектронної боротьби;
- зростання ролі і значущості протиборства в інформаційній сфері, використання новітніх інформаційних технологій (п. 20).

З огляду на такі обставини основні завдання Збройних Сил України в мирний час визначено:

- здійснення розвідувальної та інформаційно-аналітичної діяльності в інтересах оборони держави;
- здійснення заходів щодо забезпечення інформаційної безпеки (п. 23);

У п. 42 Воєнної доктрини України інформаційні ресурси названо одним із важливих джерел забезпечення діяльності Збройних Сил України, інших військових формувань та правоохоронних органів, створення умов їх ефективного функціонування.

Як бачимо, у вітчизняному законодавстві є багато нормативно-правових актів, які містять норми з визначення цілей та принципів забезпечення інформаційної безпеки. Проте деякі положення незрідка є неузгодженими й виражені в нормах-деклараціях або нормах-цілях, що не передбачають конкретних механізмів реалізації.

Зазначимо, що негативні думки щодо доцільності створення різних програм і стратегій безпеки, які так “полюбляють” в Україні, висловлювалися вже неодноразово і є досить обґрунтованими з огляду як теорії, так і практики багатьох розвинених країн. На думку одного з представників Королівської Військової Академії Великобританії, в період після холодної війни Великобританія не має стратегії національної безпеки. Те, що ми маємо, є бачення того, яку Європу ми хочемо побачити, і погляди щодо певної політики, яка може допомогти реалізувати це бачення... Але ми часто повертаємось із враженням, що в Україні переважаюче бачення безпеки є перевернутим з ніг на голову: що безпека бачиться продуктом “програм”, “стратегій”, членства у міжнародних органах та, врешті, аналізів міжурядових договорів”¹⁶². Фактично за подібними стратегіями немає ніяких конкретних практичних заходів.

¹⁶² Sherr J. Particularities and priorities of the national security strategy of UK. / Стратегія національної безпеки України в контексті досвіду світової спільноти: 3б. ст. за матер. міжнар. конф. – К. : Сатсанга, 2001. – С. 12 – 13.

У світовій практиці питання формування поглядів та підходів на вирішення актуальних питань державного життя, в т. ч. й інформаційної безпеки, традиційно вирішуються у форматі так званих Зелених та Білих книг, які створюються як державними, так і недержавними інституціями. “Зелена книга” є зібранням конкретних проблемних питань, які потребують вирішення і виносяться на обговорення чи то в органах державної влади чи то в суспільстві. У свою чергу, за результатами такого обговорення формується “Біла книга”, яка містить конкретні рекомендації щодо напрямів і способів розв’язання зазначених проблем.

У цьому аспекті цікавим є досвід Державної служби спеціального зв’язку та захисту інформації України, яка підготувала аналогічний проект під назвою “Біла книга з питань інформаційної безпеки”. Умній висвітлюються стан і перспективи вирішення всього комплексу питань, пов’язаних з інформаційною безпекою України.

Зокрема, в Білій книзі подано класифікацію основних складових інформаційної безпеки та конкретних завдань щодо їх захисту. Основними об’єктами захисту в межах інформаційної безпеки в цій класифікації є інформаційний простір, інформація з обмеженим доступом та інформаційні ресурси. Відіокремлено такі основні системоутворювальні складові інформаційної безпеки:

1) захист інформаційного простору:

- забезпечення безпеки діяльності, пов’язаної із забезпеченням свободи слова та доступу громадян до інформації;
- протидія поширенню засобами масової інформації культу насильства, жорстокості, порнографії;
- протидія намаганням маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації;
- протидія комп’ютерній злочинності та комп’ютерному тероризму;

2) захист інформації з обмеженим доступом:

- захист інформації, що становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства та держави;
- захист інформації з обмеженим доступом, що циркулює в інформаційно-телекомунікаційних системах;

3) захист інформаційних ресурсів:

- забезпечення безпеки інформаційно-телекомунікаційних систем загального призначення;
- захист національних інформаційних ресурсів, у т. ч. тих, доступ до яких здійснюється з використанням Інтернет;
- забезпечення безпеки інформаційно-телекомунікаційних систем органів державної влади та місцевого самоврядування, інформаційно-телекомунікаційних систем, які функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківських та інших сфер економіки держави, систем управління життєзабезпеченням;

5. 4. Інституціональний механізм інформаційної безпеки

Політика інформаційної безпеки реалізується як системою інститутів публічної влади, так і інститутами громадянського суспільства, до компетенції яких стосується вирішення питань щодо створення безпечних умов функціонування і розвитку інформаційної сфери. Тому одним із чинників негативного впливу на ефективність захисту інформаційної безпеки є недостатня розвиненість та інституціалізація громадянського суспільства в Україні, яке б мало бути інструментом контролю за діяльністю органів публічної влади механізмом, який забезпечує визначення й репрезентацію національних інтересів усього українського суспільства.

Основні завдання все ж вирішуються у межах формалізованої складової механізму інформаційної безпеки, яка представлена органами публічної влади. Так, багато фахівців рівень ефективності забезпечення безпеки ставлять у пряму залежність від здатності координувати зусилля різних відомств та формування певної “міжвідомчої спільноти”, діяльність якої спрямована на вирішення конкретних поставлених завдань.

Зрозуміло, що залежно від характеру завдань їх виконання є компетенцією державних органів різного рівня, які належать до різних гілок влади, мають різні сфери діяльності та обсяги владних повноважень. Та враховуючи, що політика інформаційної безпеки як суспільне явище має комплексний характер, включає внутрішньо й зовнішньополі-

тичні, економічні, технологічні, військові та інші елементи і тому потребує комплексного підходу, потрібно розглядати діяльність державних органів, спрямовану на виконання конкретних завдань у цій сфері, в межах єдиного інституціонального механізму, мета якого – забезпечити належні умови здійснення інформаційних процесів в Україні.

Отже, інституціональний механізм інформаційної безпеки – це ієрархічна сукупність органів різних гілок влади та різних рівнів, які в межах своєї компетенції вирішують конкретні завдання з формування та реалізації політики інформаційної безпеки.

Склад механізму інформаційної безпеки визначається нормами ст. 4 Закону України „Про основи національної безпеки України”:

- Президент України;
- Верховна Рада України;
- Кабінет Міністрів України;
- Рада національної безпеки і оборони України;
- міністерства та інші центральні органи виконавчої влади;
- Національний банк України;
- суди загальної юрисдикції;
- прокуратура України;
- місцеві державні адміністрації та органи місцевого самоврядування;
- Збройні Сили України, Служба безпеки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України.

Співвідношення компетенції центральних органів державної влади щодо захисту інформаційної безпеки можна визначити на основі аналізу конституційних положень, якими регулюються їх повноваження в інформаційній сфері та сфері національної безпеки.

Так, повноваження Верховної Ради у сфері національної безпеки та її інформаційної складової характеризуються тим, що основи цієї безпеки **визначаються** виключно законами України (п. 17 ст. 92 Конституції).

Президент виконує свої повноваження у сфері національної безпеки та її інформаційної складової, керуючись нормами п. 17 ст. 106 Конституції, згідно якими “здійснює керівництво у сферах національної безпеки і оборони України”, та нормами п. 1 ст. 106 Конституції, відповідно до якої **забезпечує** національну безпеку та її інформаційну складову.

Кабінет Міністрів *здійснює заходи щодо забезпечення* національної безпеки та її інформаційної складової (п. 7. ст. 115 Конституції)¹⁶³.

Отже, механізм взаємодії центральних органів державної влади полягає в тому, що Верховна Рада визначає параметри безпеки інформаційної сфери, Президент вирішує питання щодо визначення конкретних інструментів досягнення і забезпечення цих параметрів, а Кабінет Міністрів вирішує завдання щодо застосування обраного інструменту впливу на суспільні відносини і проведення в життя передбачених заходів.

Зазначимо, що останнім часом, після зміни конституційної моделі розподілу влад у бік парламентсько-президентської республіки, небезпечна колізія між повноваженнями Кабінету міністрів України та Президента України саме у сфері захисту національної безпеки. Це зумовлено існуючим концептуальним підходом до національної безпеки, за якого до цієї сфери можна віднести майже будь-які питання державного життя.

Через це виникає ситуація, в якій формується два центри виконавчої влади: один представлений Кабінетом Міністрів, який діє як вищий орган у системі органів виконавчої влади, другий – Президент і Рада національної безпеки і оборони України (РНБО), які діють як орган, що здійснює керівництво системою захисту національної безпеки. Через це неодноразово виникали протистояння з приводу повноважень та компетенцій між цими двома центрами. Тому, безумовно, потрібно вирішити цю проблему.

Характеризуючи функції державних органів, безпосередньо орієнтованих на вирішення питань інформаційної безпеки, слід звернути увагу на значні зміни у функціях та статусі Ради національної безпеки і оборони України (РНБО). Згідно зі ст. 107 Конституції України, РНБО – це “координаційний орган з питань національної безпеки і оборони при Президентові України”.

Відповідні повноваження конкретизовано і в Законі “Про Раду національної безпеки і оборони України”¹⁶⁴. Так, до основних функцій РНБО віднесено (ст. 3):

- внесення пропозицій Президентові України щодо реалізації засад внутрішньої і зовнішньої політики у сфері національної безпеки і оборони;

¹⁶³ Конституція України. Прийнята Верховною Радою України 28 червня 1996 року // Відомості Верховної Ради України. – 1996. – №30 – Ст. 141.

¹⁶⁴ Про Раду національної безпеки і оборони України: Закон України від 5 березня 1998 року № 183/98-ВР // Відомості Верховної Ради. – 1998. – № 35. – Ст. 237.

- координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони у мирний час;
- координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони в умовах воєнного або надзвичайного стану та при виникненні кризових ситуацій, що загрожують національній безпеці України.

Для виконання цих завдань РНБО наділена відповідною компетенцією. Серед повноважень цього органу, визначених ст. 4 зазначеного Закону є кілька ключових, які дозволяють РНБО активно впливати на діяльність органів виконавчої влади та місцевого самоврядування в питаннях, що стосуються сфери національної безпеки. Так, РНБО:

- розробляє та розглядає на своїх засіданнях питання, які відповідно до законодавства належать до сфери національної безпеки і оборони, та подає пропозиції Президентові України;
- здійснює поточний контроль за діяльністю органів виконавчої влади у сфері національної безпеки і оборони, подає Президентові України відповідні висновки та пропозиції;
- координує і контролює діяльність органів місцевого самоврядування в межах наданих повноважень під час введення воєнного чи надзвичайного стану.

Структура апарату РНБО та основні завдання, які вона виконує, визначені Указом Президента України “Питання Апарату Ради національної безпеки і оборони України”¹⁶⁵. Згідно з цим Указом Апарати РНБО працюють:

- Секретар РНБО
- Перший заступник Секретаря РНБО
- п’ять заступників Секретаря РНБО
- Голова Комітету з політики військово-технічного співробітництва та експортного контролю при Президентові України
- Служба Секретаря РНБО.

До структури апарату цього органу входять департаменти, служби й управління, через які здійснюється управління окремими аспектами національної безпеки: Департамент з питань воєнної безпеки, Департамент зовнішньополітичних аспектів національної безпеки, Департамент з питань економічної, соціальної та екологічної безпеки,

¹⁶⁵ Питання Апарату Ради національної безпеки і оборони України: Указ Президента України від 14 жовтня 2005 р. № 1446/2005.

Департамент з питань державної безпеки, Департамент організаційно-технічного забезпечення, Управління стратегічних розробок, Служба забезпечення діяльності Комітету з питань розвідки, Служба по зв'язках з громадськістю, Контрольне управління.

Слід зазначити про значне зростання ролі посади Секретаря РНБО в політичному й державному житті України. Ця тенденція була розпочата з 2005 р. Зокрема, згаданим вище Указом Президента України “Питання Апарату Ради національної безпеки і оборони України” Секретареві РНБО надано широкі контрольно-розпорядчі повноваження в галузі національної безпеки. Так, згідно з п. 7 цього Указу, Секретар Ради національної безпеки і оборони України:

- організовує роботу, пов'язану з підготовкою та проведенням засідань Ради та контролем за виконанням прийнятих нею рішень, а також за виконанням актів і доручень Президента України;
- порушує в установленому порядку за результатами здійснення контролю за виконанням рішень Ради питання щодо відповідальності посадових осіб;
- представляє за дорученням Голови Ради позицію Ради у Верховній Раді України, у відносинах з органами виконавчої влади та органами місцевого самоврядування, з політичними партіями і громадськими організаціями та засобами масової інформації, з міжнародними організаціями;
- вносить до органів виконавчої влади обов'язкові для розгляду пропозиції та рекомендації з питань національної безпеки і оборони, поліпшення координації заходів, що здійснюються цими органами у зазначеній сфері, тощо.

Секретар РНБО у межах своїх повноважень також має право видавати розпорядження, організовувати й контролювати їх виконання.

Питання інформаційної безпеки певною мірою вирішуються у процесі діяльності низки органів виконавчої влади, серед яких: Міністерство внутрішніх справ, Міністерство транспорту та зв'язку, Міністерство освіти і науки, Міністерство культури і мистецтв, Служба безпеки України, Департамент спеціальних телекомунікаційних систем та захисту інформації СБУ, Державний комітет з питань телебачення і радіомовлення, Державний комітет архівів, Національна Рада з питань телебачення і радіомовлення, окремі підрозділи Секретаріату Президента України та Кабінету Міністрів України, обласних дер-

жавних адміністрацій, режимно-секретні органи підприємств, установ та організацій.

Ці органи можна поділити на дві категорії: такі, для яких забезпечення інформаційної безпеки є одним з напрямів діяльності, і такі, для яких питання інформаційної безпеки є лише засобом реалізації їх головних функцій.

Працюють у цьому напрямі і різні дорадчі структури: Інститут стратегічних досліджень при Президентові України, радники, які запрошуються органами виконавчої влади, та ін.

Певні завдання щодо забезпечення інформаційної безпеки виконують підрозділи *Міністерства внутрішніх справ*¹⁶⁶.

Можна виділити три головні напрями діяльності МВС у сфері інформаційної безпеки:

- правоохоронна діяльність із дотримання норм інформаційного законодавства, яка полягає у: запобіганні злочинам та правопорушенням в інформаційній сфері, їх припиненні, розкритті й розслідуванні, вжитті заходів до усунення причин і умов, що сприяють вчиненню правопорушень;
- забезпечення фізичного захисту і оборони силами міліції та внутрішніх військ об'єктів інформаційної інфраструктури, що перебувають у державній власності, та охорона на договірних засадах об'єктів інформаційної інфраструктури, що перебувають у приватній власності;
- безпосереднє інформаційно-аналітичне забезпечення діяльності, пов'язаної з боротьбою із злочинністю, охороною громадського порядку, забезпеченням громадської безпеки тощо. Це, зокрема, формування довідково-інформаційних фондів, ведення оперативно-пошукового та криміналістичного обліку, складання певних видів державної статистичної звітності та ін.

Важливі завдання інформаційної безпеки, безперечно, виконує *Служба безпеки України*, яка, згідно з нормами ст. 1 Закону “Про службу безпеки України” визначається як “державний правоохоронний орган спеціального призначення, який забезпечує державну безпеку України”¹⁶⁷.

Сворена у 2006 р. *Державна служба спеціального зв'язку та захисту інформації України*, яка є державним органом, що призна-

¹⁶⁶ Про затвердження положення про Міністерство внутрішніх справ України: Постанова Кабінету Міністрів України від 4 жовтня 2006 р. № 1383.

¹⁶⁷ Про Службу безпеки України: Закон України від 25 березня 1992 р. № 2229-XII // Відомості Верховної Ради України. – 1992. – № 27. – Ст. 382.

чений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації¹⁶⁸.

Для забезпечення ефективного контролю діяльності цієї служби та створення належних умов для виконання покладених на неї завдань, законодавство передбачає досить складну систему організації управління нею, в якій бере участь Кабінет Міністрів, Верховна Рада та Президент України:

- діяльність Державної служби спеціального зв'язку та захисту інформації України спрямовується Кабінетом Міністрів України, який здійснює заходи щодо забезпечення її функціонування;
- Державна служба спеціального зв'язку та захисту інформації України підконтрольна Верховній Раді України;
- з питань, пов'язаних із забезпеченням національної безпеки України, Державна служба спеціального зв'язку та захисту інформації України підпорядковується і підконтрольна Президентові України.

Недержавні суб'єкти – *громадські об'єднання та організації, суб'єкти підприємницької діяльності* тощо, відповідно до законодавства, зокрема норм ст. 505 ЦК України¹⁶⁹, самостійно вживають заходів захисту власної інформаційної безпеки і відповідно самостійно визначають організаційні форми цього захисту, крім випадків, коли подібні заходи визначаються законодавством.

Специфіка застосування форм і методів державного управління у сфері інформаційної безпеки зумовлена потребами поєднання відкритості і конфіденційності в інформаційних відносинах і полягає в необхідності забезпечення балансу між інформаційними правами і свободами людини та завданнями держави щодо захисту інформації, регулювання доступу до неї та її збирання, використання і поширення. Важливим є також вплив процесів інформатизації на зміст управлінської діяльності, підвищення ролі інформаційного забезпечення у прийнятті рішень, інформаційної діяльності як одного із важелів управлінського впливу.

¹⁶⁸ Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23 лютого 2006 р. № 3475-IV // Відомості Верховної Ради України. – 2006. – № 30. – Ст. 258.

¹⁶⁹ Цивільний кодекс України від 16 січня 2003 р. // Відомості Верховної Ради України. – 2003. – № 40 – 44. – Ст. 356.

5. 5. Міжнародно-правові засади інформаційної безпеки.

Однією із найактуальніших і найнебезпечніших загроз, яку несе в собі розвиток інформаційних технологій, є проблема інформаційних війн та інформаційного тероризму. Попри існування багатьох спільних ознак між інформаційними війнами та інформаційним тероризмом (адже і в тому і в тому випадку відбувається несанкціоноване, протиправне втручання в інформаційні процеси), а різниця полягає насамперед у суб'єкті цих дій (держава або кримінальні чи терористичні угруповання) питання інформаційного тероризму набуло більш широкого визнання на міжнародному рівні, тоді, як питання інформаційних війн та інформаційної зброї незрідка залишалося за рамками обговорень. Так, ще в 1996 р. в Резолюції Організації Об'єднаних Націй 51/210 “Заходи щодо ліквідації міжнародного тероризму” (п 3. (с)) державам пропонувалося, під час здійснення заходів боротьби з тероризмом, у т. ч. при створенні відповідного законодавства, “звернути увагу на ризик використання терористами електронних або дрових комунікацій для вчинення кримінальних дій і необхідність знайти засоби, погоджені з національним законодавством, для запобігання подібній злочинності і розвитку відповідної співпраці”¹⁷⁰.

Правові питання боротьби з інформаційним тероризмом почали прушувати на Нараді на рівні міністрів з проблеми тероризму (*Ministerial Conference on Terrorism*), що відбулася 30 липня 1990 р. в Парижі в межах Загальноамериканської спеціалізованої конференції з тероризму (*Inter-American Specialized Conference on Terrorism*), яка проходила в Лімі 23 – 26 квітня 1996 р. під егідою Організації американських країн, і відтоді стали неодмінним аспектом розгляду проблеми тероризму взагалі.

Правові проблеми інформаційної війни та регулювання застосування інформаційної зброї, навпаки тривалий час у сфері відкритої інформації були лише предметом наукових дискусій. Тому найактивнішу роль у винесенні на порядок денний міжнародної спільноти всього комплексу питань інформаційної безпеки відігравала і продовжує відігравати Російська Федерація, яка, зокрема, була ініціатором розгляду цих питань у рамках ООН.

¹⁷⁰ United Nations. A/RES/51/210. “Measures to eliminate international terrorism” Resolution Adopted By The General Assembly. 17 December 1996.

Саме з ініціативи Росії цю проблему було офіційно визнано на міжнародному рівні, коли 4 січня 1999 р. на 53 сесії Генеральної Асамблеї ООН було прийнято резолюцію 53/70 “Досягнення у сфері інформатизації і телекомунікації в контексті міжнародної безпеки”¹⁷¹. В цій Резолюції було висловлено стурбованість тим, що новітні інформаційні технології і засоби телекомунікації можуть бути використані в цілях, несумісних із завданнями забезпечення міжнародної стабільності і безпеки, і можуть негативно вплинути на безпеку держав; підкреслено необхідність попередження неправомірного використання або використання інформаційних ресурсів чи технологій у злочинних або терористичних цілях і у зв’язку з цим зроблено заклик держав-членів ООН сприяти розгляду на багатосторонньому рівні існуючих і потенційних загроз у сфері інформаційної безпеки.

На думку деяких фахівців, прийняття такої резолюції Генеральною Асамблеєю ООН виявилось як ніколи своєчасним. Оскільки на той час (1999 р.) “існували не лише значні напрацювання у сфері створення засобів впливу на інформаційний ресурс, а й численні факти військового застосування засобів, які інакше як інформаційною зброєю не назвеш. За деякими даними, розробки таких засобів здійснюються у 120 країнах світу. Крім того, в деяких країнах розробляються засоби інформаційного протидіювання з вірогідними противниками як в умовах воєнних конфліктів різного ступеня інтенсивності, так і в мирний час, тобто в умовах ведення так званої інформаційно-психологічної війни”¹⁷².

Зокрема, міністерство оборони США одним із перших видало офіційний документ, директиву Т 3600 “Інформаційна війна”, ще 21.12.2001 р. А офіційне визначення інформаційної війни було дано ще в 1997 р. як дії, вжиті для досягнення інформаційної переваги в інтересах національної стратегії і які реалізуються через вплив на інформацію в інформаційні системи противника при одночасного захисту власної інформації та власних інформаційних систем¹⁷³.

Специфіка інформаційної зброї в тому що об’єктом її застосування може бути будь-який із трьох елементів інформаційної сфери: “За-

¹⁷¹ United Nations. A/RES/53/70 “Developments in the field of information and telecommunications in the context of international security” Resolution Adopted By The General Assembly. 4 January 1999.

¹⁷² Смирнов А. И. Некоторые проблемы международной информационной безопасности // Юрид. мир. – 2001. – авг. – с. 16 – 17.

¹⁷³ Панарин И. Информационная война XXI века: готова ли к ней Россия // Власть. – 2000. – № 2. – С. 105.

соби і лінії зв'язку – матеріальна основа світової інформаційної інфраструктури (до неї належать не лише засоби, поєднані між собою різними каналами зв'язку, а й уся апаратура, призначена для обробки інформації); інформація в чистому вигляді ті її потоки; сама людина”¹⁷⁴. Таким чином, застосування інформаційної зброї охоплює:

- деструктивний вплив на матеріальні об'єкти інформаційної сфери;
- знищення, спотворення або зміну інформації;
- цілеспрямований вплив на нервову систему, психіку та свідомість людини.

Застосування такої зброї може бути як відкритим в умовах відкритого збройного конфлікту, так і латентним у межах інформаційного протиборства в мирний час.

Починаючи з 53-сесії ООН (1999 р.) питання досягнень у сфері інформатизації й телекомунікації в контексті міжнародної безпеки вносяться до порядку денного кожної наступної сесії цієї організації. Відповідно питання міжнародної інформаційної безпеки ставали предметом обговорення на сесіях Генеральної Асамблеї ООН, і з цих питань було прийнято резолюції 54/40 (23 грудня 1999 р)¹⁷⁵ та 55/28 (20 грудня 2000 р.)¹⁷⁶. В цих резолюціях, зокрема, пропонувалося державам – членам ООН продовжувати інформувати Генерального Секретаря про власний погляд на загальне оцінювання проблем інформаційної безпеки, визначення основних понять у цій сфері та змісту відповідних міжнародних концепцій, спрямованих на зміцнення безпеки глобальних інформаційних та телекомунікаційних систем.

Під час обговорення відповідного пункту порядку денного на 56-й сесії Генеральної Асамблеї у доповіді Генерального Секретаря було наведено позиції, висловлені деякими державами щодо сутності питань міжнародної інформаційної безпеки. Зокрема, уряд Філіппін запропонував визначати основні поняття в рамках інформаційної безпеки:

Інформаційна зброя – інформаційні ресурси, стратегічно розроблені або створені для ведення інформаційної війни або для завдан-

¹⁷⁴ Петров В. , Рабинович И. От информационных войн к управляемому информационному сотрудничеству // Власть. – 2001. – № 1. – С. 21 – 22.

¹⁷⁵ United Nations. A/RES/54/40 “Developments in the field of information and telecommunications in the context of international security” Resolution Adopted By The General Assembly. 23 December 1999.

¹⁷⁶ United Nations. A/RES/55/28 “Developments in the field of information and telecommunications in the context of international security” Resolution Adopted By The General Assembly. 20 December 2000.

ня шкоди, збентеження, створення незручностей або будь-яких інших дій зловмисного характеру.

Інформаційна війна: 1) дії з метою досягнення інформаційної переваги застосуванням заходів для експлуатування, підриву, знищення, дестабілізації та руйнування інформаційного потенціалу противника і його функцій; 2) заходи захисту власних інформаційних ресурсів і телекомунікаційних систем; 3) дії з метою використання інформаційних ресурсів і телекомунікаційних систем іншої сторони для досягнення цілей та інтересів, наприклад електронна війна (інформаційна війна в оборонному і військовому контексті), війна в Інтернеті (інформаційна війна в більш широкому суспільному контексті).

Інформаційний тероризм. Терористичні дії в контексті інформаційної безпеки”¹⁷⁷.

Заслугує на увагу і наведена в цій доповіді спільна позиція країн — членів Європейського Союзу, яка була висловлена представником Швеції. У рамках цієї позиції ЄС визнає існування потенційної небезпеки несанкціонованого втручання або протиправного використання інформаційних і телекомунікаційних технологій, але разом з тим підкреслює, що такі технології сприяють вільному потоку інформації і створюють величезні вигоди для окремих осіб, підприємців і урядів у усьому світі, сприяють розвитку демократії і свободи слова, прогресу громадянського суспільства. Щодо основних понять, то вони були сформульовані так:

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

Інформаційна безпека також охоплює захист інформації, що стосується військового потенціалу та інших аспектів національної безпеки. Недостатній захист життєво важливих інформаційних ресурсів та інформаційних і телекомунікаційних систем може створити загрозу для міжнародної безпеки”. Однак, підкреслюючи значення міжнародної співпраці у вирішенні питань інформаційної безпеки, країни ЄС вважають, що “в першу чергу кожна держава має право і несе відповідальність за захист своєї інформації і систем, що базуються на інформації” і зазнача-

¹⁷⁷ 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.

ють, що Генеральна Асамблея не повинна бути “основним форумом для розгляду цих питань”¹⁷⁸. Отже ЄС наголошує на існуванні проблеми балансу між питаннями інформаційної безпеки і питаннями свободи слова та вільного руху інформації. Крім того, як не дивно, було обійдеться питання однієї з найбільших загроз інформаційній безпеці, а саму інформаційну безпеку визначено насамперед внутрішньодержавною справою.

Росія, навпаки, акцентувала увагу саме на військових аспектах інформаційної безпеки, накресливши у своїх пропозиціях, що були подані в Додатку № 1 до доповіді Генерального секретаря, власну класифікацію видів інформаційної зброї, до якої увійшли:

- електронні або психічно-електронні засоби, що використовуються незаконними (неконституційними) військовими організаціями, терористичними групами або особами для тимчасової чи постійної нейтралізації електронних установок або систем;
- засоби впливу на програмні ресурси електронних засобів контролю з метою їх руйнування або зупинення їх операційних алгоритмів;
- засоби впливу на процеси передачі інформації з метою їх зупинки або зламу шляхом втручання у середовище розповсюдження сигналу або алгоритм функціонування;
- засоби поширення дезінформації або створення в інформаційному середовищі віртуальної картини, що повністю або частково змінює уявлення реальності;
- засоби дії на людську свідомість та мислення з метою дезорієнтації, втрати сили волі або часткової дестабілізації.

Під час обговорення доповіді Генерального Секретаря та доповіді Першого комітету¹⁷⁹ Генеральна Асамблея сформулювала низку пропозицій, які дістали відображення в ухваленій Резолюції Генеральної Асамблеї ООН 56/19, в якій намагалися врахувати позиції всіх сторін¹⁸⁰.

Так, було запропоновано (п. 1) і надалі сприяти розгляду на багатосторонньому рівні існуючих і потенційних загроз у сфері інформаційної безпеки, а також можливих заходів з обмеження загроз, що

¹⁷⁸ 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.

¹⁷⁹ Developments in the field of information and telecommunications in the context of international security / Fifty-six session. Report of the First Committee. 14 November 2000. United Nations. A/56/533.

¹⁸⁰ United Nations. A/RES/56/19 “Developments in the field of information and telecommunications in the context of international security” Resolution Adopted By The General Assembly. 7 January 2002.

виникають у цій сфері, зважаючи на необхідності зберегти вільний рух інформації. Тобто основним принципом створення міжнародних концепцій інформаційної безпеки було визнано *принцип додержання необхідного балансу між заходами безпеки в інформаційній сфері та принципом свободи інформації*.

Разом з тим було внесено пропозицію Генеральному Секретареві (п. 4) провести дослідження концепцій міжнародної інформаційної безпеки за допомогою групи експертів, призначених ним на основі справедливого географічного розподілу урядових експертів (яку було створено в 2004 р.), а також за сприяння держав, що можуть його надати, і таким чином створено передумови для міжнародно-правової оцінки цієї проблеми.

Значним кроком у створенні міжнародно-правових засад захисту інформаційної безпеки стало підписання в рамках Ради Європи Конвенції про кіберзлочинність (23 листопада 2001 р., Будапешт) Україна ратифікувала цю Конвенцію у 2005 р.¹⁸¹. Цей міжнародно-правовий акт установлює певну систему правил щодо визначення видів з використанням інформаційних та телекомунікаційних технологій, які країни – сторони цієї Конвенції зобов'язані імплементувати в національне законодавство. Конвенція визначає декілька груп правопорушень у цій сфері. Так, усі “кібернетичні” правопорушення поділено на п'ять груп, у межах яких виділено окремі їх види.

Першу групу названо “Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем”. Вона охоплює такі дії, як незаконний доступ, нелегальне перехоплення; втручання у дані, втручання в систему, зловживання пристроями.

Другу групу становлять “Правопорушення, пов'язані з комп'ютерами” підробка, пов'язана з комп'ютерами, та шахрайство, пов'язане з комп'ютерами (мається на увазі створення або підміна даних із злочинною метою).

Третя група це – “Правопорушення, пов'язані зі змістом”, до якої належать правопорушення, пов'язані з дитячою порнографією.

Нарешті, четверту групу становлять “Правопорушення, пов'язані з порушенням авторських та суміжних прав”.

Отже, можна говорити про поступовий розвиток міжнародно-правових стандартів у галузі інформаційної безпеки, які мають важ-

¹⁸¹ Конвенція про кіберзлочинність. Рада Європи. Будапешт 23 листопада 2001 р. (Ратифіковано Законом України “Про ратифікацію Конвенції про кіберзлочинність” від 7 вересня 2005 р. № 2824-IV).

ливе значення для інформаційної безпеки національних держав, враховуючі сучасні тенденції глобалізації та інформатизації. Існує нагальна потреба у більш широкому сприйнятті Україною цих стандартів, зокрема створених у рамках програм та планів Європейського Союзу з формування Єдиного європейського інформаційного простору.

Використання зарубіжного досвіду при формуванні національного державно-правового механізму інформаційної безпеки дасть змогу уникнути так популярного в нашій країні процесу “винаходу велосипеда”, оскільки у світі існує досить багато країн з більш високим рівнем інформатизації, які раніше зіткнулися з тими проблемами, що нині постають перед Україною. Найбільш прийнятні організаційно-правові підходи до проблеми реалізовані законодавством США, Канади, країн – членів Європейського Союзу, Російської Федерації. При цьому йдеться як про запозичення конструктивного досвіду, так і про відмову від кроків, що призводять до негативних наслідків в інформаційній сфері.

ГЛАВА 6. ПРАВОВІ РЕЖИМИ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНИХ РЕСУРСІВ

Поняття і правовий режим інформаційних ресурсів. Режим доступу до інформації: поняття і зміст. Основні принципи правового регулювання обігу інформації. Обмеження в розповсюдженні інформації

6. 1. Поняття і правовий режим інформаційних ресурсів.

З огляду на нематеріальний характер інформації, однією із важливих умов виникнення правових відносин щодо неї є встановлення певної сукупності правил, що визначають правовий статус конкретної інформації та її матеріальних носіїв. Так, останнім часом значна увага приділяється питанням *правового регулювання* формування та функціонування *інформаційних ресурсів*, а сам цей термін почали широко використовувати в національному законодавстві. Одне з перших тлумачень поняття “інформаційний ресурс” було запроваджено нормами ч. 1 ст. 10 Закону України “Про науково-технічну інформацію”, згідно з якою інформаційні ресурси – це “сукупність довідково-інформаційних фондів з необхідним довідково-пошуковим апаратом і відповідними технічними засобами зберігання, обробки і передачі, що є у володінні, розпорядженні, користуванні державних органів і служб науково-технічної інформації, наукових і науково-технічних бібліотек, комерційних центрів, підприємств, установ і організацій”¹⁸².

Таким чином, було запроваджено комплексний підхід до поняття “інформаційний ресурс”, згідно з яким останній складається з двох взаємопов’язаних елементів: безпосередньо інформації (сукупність довідково-інформаційних фондів) та певна інформаційна система, що забезпечує користування цим ресурсом (довідково-пошуковий апарат і технічні засобами зберігання, обробки і передачі).

¹⁸² Про науково-технічну інформацію: Закон України № 3322-XII від 25 червня 1993 р. // Відомості Верховної Ради України. – 1993. – № 33. – Ст. 345.

Найбільш універсальне визначення інформаційного ресурсу міститься в Законі України “Про національну програму інформатизації”¹⁸³. Згідно зі ст. 1 Закону, *інформаційний ресурс – це сукупність документів в інформаційних системах*. Крім того, цією нормою визначаються основні види інформаційних систем, які забезпечують існування й доступ до інформаційних ресурсів, до яких належать: *бібліотеки, архіви, банки даних тощо*.

На жаль, у національному законодавстві немає єдиного визначення правового режиму інформаційних ресурсів, а більшість нормативно-правових актів регулюють правові режими інформаційних ресурсів в окремих інформаційних системах. Проте саме єдиний правовий режим може бути тією універсальною характеристикою, що об’єднує окремі документи в цілісну інформаційну систему.

Така концепція набула широкого визнання в науковій літературі, де вже достатньо давно використовується поняття *правовий режим інформаційних ресурсів*, яким характеризується сукупність правових норм, що регулюють суспільні відносини щодо того чи іншого інформаційного ресурсу. “Правові норми в даному випадку встановлюють обов’язкові вимоги, без яких інформаційний ресурс не можна включити до системи правових відносин і отримати повноцінні гарантії в процесі взаємодії суб’єктів з приводу конкретних об’єктів даного ресурсу”¹⁸⁴.

Для більш чіткого розуміння змісту й сутності поняття „інформаційні ресурси” та їх правового режиму звернімося до підписано у рамках СНД Угоди “Про правовий режим інформаційних ресурсів Прикордонних військ держав–членів Співдружності Незалежних Держав”¹⁸⁵. Щоправда, Україна від підписання цієї угоди утрималась, а сама угода виражає переважно концептуальні положення правового регулювання інформаційних ресурсів, що застосовуються в законодавстві Російської Федерації.

Ця угода (ст. 1) визначає інформаційні ресурси як *оброблену у визначеному порядку сукупність документованої інформації в інформаційних системах*. Відповідно сам документ – це засіб документу-

¹⁸³ Про Національну програму інформатизації: Закон України від 4 лютого 1998 р. № 74/98-ВР // Відомості Верховної Ради України. – 1998. – № 27–28. – Ст. 18.

¹⁸⁴ Бачило І. Л. Информационное право. Основы практической информатики. – М., 2001. – С. 99.

¹⁸⁵ Соглашение о правовом режиме информационных ресурсов Пограничных войск государств-участников Содружества Независимых Государств (Москва, 25 ноября 1998 г.) // Содружество. Инф. вест. Совета глав государств и Совета глав правительств СНГ. – № 3(30). – С. 299 - 304.

вання, що містить у зафіксованому вигляді згідно зі встановленими формами і правилами інформацію, необхідну для реалізації інформаційних процесів.

Крім того, слід зважити ще на такі два важливих для розуміння змісту поняття інформаційні ресурси, визначення:

- *матеріальний носій інформації* – матеріал із певними фізичними властивостями, який може бути використаний для запису і зберігання інформації;
- *документована інформація* – зафіксована на матеріальному носії інформація з реквізитами, що дають змогу її ідентифікувати.

Як уже зазначалося, правовий режим інформаційного ресурсу складається з правових норм, що визначають ключові правила, за якими той чи той інформаційний ресурс може бути залучений в обіг інформації в суспільстві.

Такими нормами, є:

- 1) право власності на інформацію, окремі документи та масиви документів в інформаційних системах;
- 2) порядок документування інформації, надання документам юридичної сили та її підтвердження;
- 3) категорії інформації відповідно до рівня доступу до неї;
- 4) мета й порядок захисту інформації;
- 5) права суб'єктів, що беруть участь в інформаційних відносинах щодо певного інформаційного ресурсу.

Право власності на інформацію в межах інформаційного ресурсу є складною категорією, адже в рамках одного інформаційного ресурсу може бути використана інформація, права на яку належать різним особам. Це стосується як окремих документів, так і конкретної інформації (даних), що міститься в кожному з документів.

За Законом України “Про інформацію”¹⁸⁶ (ст. 38), право власності на інформацію – це врегульовані законом суспільні відносини з володіння, користування й розпорядження інформацією.

Інформація є об'єктом права власності громадян, організацій (юридичних осіб) і держави. Вона може бути таким об'єктом права як у повному обсязі, так і об'єктом лише володіння, користування чи розпорядження.

Підставами виникнення права власності на інформацію є:

¹⁸⁶ Про інформацію: Закон України від 2 жовтня 1992 р. // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

- 1) створення інформації своїми силами і своїм коштом;
- 2) договір на створення інформації;
- 3) договір, що містить умови переходу права власності на інформацію до іншої особи.

Важливим є також право власності на *масиви документів в інформаційних системах*, (ст. 40, 41 Закону України “Про інформацію”).

Результатами інформаційної діяльності можуть бути:

- інформаційна продукція – матеріалізований результат інформаційної діяльності, призначений для задоволення інформаційних потреб громадян, державних органів, підприємств, установ і організацій;
- інформаційна послуга – здійснення у визначеній законом формі інформаційної діяльності з доведення інформаційної продукції до споживачів з метою задоволення їх інформаційних потреб.

Таким чином, інформаційних ресурс загальною, як сукупність документів, також є об’єктом права власності, яке може відрізнятися від прав власності на окремі документи, що містяться в ньому.

Не менш важливим у правовому режимі інформаційного ресурсу є *порядок документування інформації та інколи порядок надання документам юридичної сили та її підтвердження*. Порядок документування інформації визначає форму подання документа і вид фізичного носія, на якому його закріплено. Найбільш поширеними носіями документів є паперові, магнітні та оптичні носії. Відповідно, документи можуть бути друковані, рукописні, аудіо, візуальні чи електронні. На носії та форми подання документів встановлені певні технічні стандарти. Порядок надання документам юридичної сили передбачає наявність у документі визначених законодавством *обов’язкових реквізитів*, за якими можна визначити авторство, цілісність та достовірність документа.

Інформаційні ресурси поділяють залежно від *категорії інформації за доступом до неї*. Ці категорії зумовлені режимом доступу до інформації та її матеріальних носіїв, що містяться в конкретному інформаційному ресурсі. За режимом доступу до інформації інформаційні ресурси поділяються на:

- *відкриті* – інформаційні ресурси загального користування, які створюються для задоволення інформаційних потреб суспільства і право доступу до яких мають будь-які фізичні або юридичні особи;

- з обмеженим доступом – інформаційні ресурси, які використовують органи публічної влади, підприємства, установи та організації і їх посадові особи та працівники, відповідно до законодавства і з метою виконання обов’язків та завдань, віднесених до їх компетенції.

З огляду на потребу у забезпеченні права власності на інформаційний ресурс та режими доступу до інформації, що міститься в інформаційному ресурсі, визначають і *мету і порядок захисту інформації*, що відображує діяльність, спрямовану на запобігання несанкціонованим діям щодо інформаційного ресурсу.

Для інформаційних ресурсів загального доступу основною метою захисту інформації є запобігання її блокуванню порушенню цілісності або знищенню інформації.

Для інформаційних ресурсів з обмеженим доступом, крім зазначеного вище, важливим є запобігання *витоку інформації*, тобто несанкціонованих дій, внаслідок яких інформація стає відомою чи доступною особам, що не мають права доступу до неї.

Залежно від мети захисту інформації визначають порядок її захисту, тобто заходи її правового, організаційного, технічного та криптографічного захисту.

Введення інформаційного ресурсу в обіг неможливе без установлення *прав суб’єктів, що беруть участь в інформаційних відносинах щодо даного інформаційного ресурсу*. Такими суб’єктами, можуть бути: власник інформації, власник інформаційного ресурсу, адміністратор інформаційного ресурсу та користувач інформаційного ресурсу.

Власником інформації є особа, наділена правами володіння, користування та розпорядження інформацією, що залучено до інформаційного ресурсу. Він має право вживати певних заходів для реалізації та забезпечення своїх прав і законних інтересів, зокрема, укладенням відповідних угод із власником інформаційного ресурсу, якими визначаються права останнього щодо використання інформації та її розповсюдження.

Власник інформаційного ресурсу – це особа у власності якої є сукупність (зібрання) окремих документів та інформаційна система, що становлять інформаційний ресурс. Він визначає організаційні та методологічні принципи створення інформаційного ресурсу, ухвалює рішення про залучення окремих відомостей і документів до інформа-

ційного ресурсу, опрацьовує їх, ідентифікує, класифікує, відповідає за зміст документів, забезпечує їх зберігання і доступ до них, здійснює контроль за порядком користування інформаційним ресурсом та ін.

Адміністратор інформаційного ресурсу – це уповноважена власником цього ресурсу особа, яка здійснює супровід інформаційної системи, що є основою інформаційного ресурсу; відповідає за його функціонування, збереження даних і захист їх від руйнування, технічну підготовку документів для внесення їх до інформаційного ресурсу; здійснює обслуговування, веде облік користувачів інформаційного ресурсу та організовує контроль доступу до нього.

Користувач інформаційного ресурсу – будь-яка юридична або фізична особа, якій надано право доступу до інформаційного ресурсу. Користувач має право отримувати відомості й документи з інформаційного ресурсу та несе відповідальність за дотримання правил користування інформаційним ресурсом і використання отриманої інформації.

6. 2. Режим доступу до інформації: поняття і зміст.

Ще однією особливістю правового регулювання обігу інформації є те, що залежно від типу інформації існують і відповідні, специфічні правила поведінки при виконанні інформаційної діяльності, встановлені правовими нормами. Законом України “Про інформацію” (ст. 28) такі правила поведінки визначають як режими доступу до інформації. Згідно з нормами цієї статті, *“режим доступу до інформації – це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації”*¹⁸⁷. За своїм значенням режим доступу є однією із головних юридичних характеристик інформації, адже ним визначаються конкретні групи правових норм, що застосовуються до тієї чи іншої документованої або оприлюдненої інформації.

За своєю сутністю режим доступу до інформації є різновидом спеціальних правових режимів, які становлять “сукупність правил, закріплених в юридичних нормах, які регулюють певну діяльність людей”¹⁸⁸. Правові режими існують у межах багатьох галузей права. Оскільки вже було зазначено, що захист інформації в цілях інфор-

¹⁸⁷ Про інформацію: Закон України від 2 жовтня 1992 р. // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

¹⁸⁸ Бахрах Д. Н. Административное право: Учебник для вузов. – М.: БЕК, 1999. – С. 202

маційної безпеки здійснюється на основі імперативного методу правового регулювання, то відповідні режими доступу до інформації за своїми характеристиками є найбільш близькими до адміністративно-правових режимів.

Особливою ознакою режиму доступу до інформації є специфіка його об'єкта – *правові відносини, що виникають з приводу отримання, збереження, використання та розповсюдження інформації*.

Головними характеристиками режиму доступу до інформації є:

- суб'єкт визначення доступності цієї інформації;
- коло суб'єктів, які мають доступ до цієї інформації;
- особливі вимоги і правила зберігання та поширення цієї інформації;
- строк дії режиму.

Суб'єктом визначення доступності інформації є особа, до компетенції якої належить вирішення питань щодо встановлення обмежень на доступ до інформації та її матеріальних носіїв, а також надання права доступу до такої інформації.

Суб'єкт, що має доступ до інформації, – це особа, якій надано право ознайомлення з матеріальними носіями інформації або їх використання. Надання особі права доступу до інформації з обмеженим доступом зазвичай пов'язане із взяттям нею на себе зобов'язань щодо нерозголошення отриманої інформації.

Режим доступу до інформації означає певну сукупність правил, якими окреслено *особливі вимоги і правила зберігання та поширення інформації*. Ці правила визначають діяльність осіб, на яких покладена відповідальність за зберігання матеріальних носіїв інформації, установлюють необхідність застосування певних правових, організаційних, технічних та криптографічних засобів захисту інформації. Ці правила також визначають порядок надання доступу до такої інформації.

Нарешті, більшість видів інформації з обмеженим доступом мають визначений законодавством або власником інформації *строк дії режиму обмеження доступу до інформації*. Цей строк визначають, як правило, під час ухвалення рішення про обмеження доступу до інформації або її матеріальних носіїв. Після закінчення цього строку може бути прийняте рішення або про його поновлення, або про надання інформації статусу відкритої.

Режим доступу до інформації можна також розглядати в рамках правового режиму інформаційних ресурсів, як невід'ємну складову

останнього. Проте, саме режим доступу є універсальною характеристикою інформації, оскільки властивий будь-якій інформації, яку введено в обіг.

Режим доступу до інформації не залежить від порядку документування та форми подання інформації.

Режимом доступу до інформації визначаються права і обов'язки суб'єктів інформаційних відносин щодо отримання й поширення інформації.

Нарешті, установлення режиму обмеження доступу до інформації тягне за собою застосування таких механізмів правового захисту інформації, як установлення юридичної відповідальності за несанкціоновані дії з такою інформацією.

Згідно із Законом України “Про інформацію” (ст. 28), за режимом доступу інформація поділяється на відкриту та з обмеженим доступом. Основними ознаками *відкритої інформації* є те, що доступ до неї надається будь-яким зацікавленим особам, а будь-яке обмеження права на одержання відкритої інформації забороняється.

Закон (ст. 29) також передбачає способи забезпечення доступу до відкритої інформації:

- систематична публікація її в офіційних друкованих виданнях (бюлетенях, збірниках);
- поширення її засобами масової комунікації;
- безпосереднє надання її зацікавленим громадянам, державним органам та юридичним особам.

Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну і таємну (ст. 30 Закону України “Про інформацію”).

Конфіденційна інформація – це відомості, якими володіють, користуються або розпоряджаються окремі фізичні чи юридичні особи і поширюються за їх бажанням відповідно до передбачених ними умов.

До *таємної* належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі.

Основними характеристиками таємної інформації є те, що: віднесення її до категорії таємних відомостей, доступ до неї громадян, порядок обігу та захисту, порядок і терміни її оприлюднення визначаються законодавством.

Отже, основою класифікації інформації з обмеженим доступом виступає *суб'єкт визначення доступності інформації*.

Обмеження доступу до конфіденційної інформації належить до компетенції власника цієї інформації або особи, що має право розпоряджатися цією інформацією на законних підставах. Ці особи на власний розсуд визначають як режим обмеження доступу до інформації так і суть цього режиму, зокрема, і потребу застосуванні засобів захисту інформації та визначенні порядку надання доступу до неї. Законодавство ж встановлює права осіб на встановлення обмежень доступу до інформації, юридичну відповідальність за порушення та зловживання цим правом, категорії інформації, доступ до якої не може бути обмежений.

Обмеження доступу до *таємної інформації* встановлюється законодавством у разі відповідності інформації певним критеріям. Засекречується інформація незалежно від бажання чи небажання її власника, понад те власник інформації зобов'язаний реалізовувати своє право власності на інформацію з урахуванням встановлених законодавством обмежень, а у разі їх порушення може бути позбавлений права власності на інформацію та її матеріальні носії. Рішення про засекречування інформації ухвалюють уповноважені органи державної влади, а зміст режиму доступу до інформації, засоби її захисту та юридична відповідальність за порушення режиму визначаються законодавством.

Законодавство установлює певні обмеження щодо дотримання режиму обмеження доступу до інформації з міркувань суспільного блага. Так, згідно з ч. 11 ст. 30 Закону України “Про інформацію”, “інформація з обмеженим доступом може бути поширена без згоди її власника, якщо ця інформація *є суспільно значимою*, тобто якщо вона *є предметом громадського інтересу* і якщо *право громадськості знати цю інформацію переважає право її власника на її захист*”. Питання про відповідні умови для поширення інформації з обмеженим доступом без згоди її власника та звільнення від відповідальності осіб, що поширили цю інформацію, вирішуються в судовому порядку.

6. 3. Основні принципи правового регулювання обігу інформації.

Проблеми застосування обмежень доступу та поширення інформації можна цілком справедливо вважати найбільш давнім напрямом інформаційної безпеки держави. Від самого виникнення такого інституту, як держава, почала поширюватися практика оголошення різних відомостей таємними та конфіденційними або встановлення обмежень на їх вільне розповсюдження. Не втрачає актуальності ця проблема і в наш час.

Для чіткого визначення правової природи подібних заборон і обмежень потрібно визначитися з основними принципами обігу інформації в суспільстві, зумовленого низкою чинників.

По перше, це *природні фактори*, тобто різні фізичні й фізіологічні закони, які впливають на обіг інформації. До фізичних факторів наприклад, належать: значення швидкості світла, якою обмежуються передача даних за допомогою електронних засобів комунікації; фізичні якості фізичних носіїв інформації, які зумовлюють строк зберігання інформації на цих носіях, можливість її зміни тощо. Діють також, фізіологічні закони, які характеризують властивості індивіда як носія інформації: рівень його інтелекту, який визначає можливості збирання і обробки інформації, його здатність до забування, чим окреслюється строк, за який інформація може залишатися точною без збереження її на фізичних носіях, та ін.

Велике значення для обігу інформації в суспільстві мають *суспільні закони*: норми моралі та норми права. Саме ці норми визначають основні характеристики процесів, які прийнято називати інформаційними відносинами, що виникають між різними учасниками: фізичними та юридичними особами і державою. Інформаційні відносини – це “процеси створення, збору, обробки, накопичення, зберігання, пошуку, розповсюдження і споживання інформації”¹⁸⁹.

Інформаційні відносини, оскільки суб'єктами передачі інформації в них виступають як індивіди, так і соціальні групи, безумовно, є різновидом суспільних відносин. У цьому разі актуальним є також загальне правило стосовно охорони державою найбільш важливих видів суспільних відносин, що набувають підвищеного суспільного значення. Тому держава встановлює відповідні правові норми,

¹⁸⁹ Копылов В. А. Информационное право. – М. : Юрист, 1997. – С. 171–172.

якими регламентуються права, обов'язки та правила поведінки їх учасників.

Отже, врегульованість певних видів інформаційних відносин правовими нормами безпосередньо пов'язана із суспільним значенням конкретних видів інформації, щодо якої вони виникають. Ці правові норми регламентують насамперед параметри інформаційних процесів, за якими відбувається обіг інформації в людському суспільстві. Безумовно, що обіг різних видів інформації (зокрема, відкритої та з обмеженим доступом) регулюється різними правовими нормами, які відповідають їхній специфіці. Залежно від виду інформації законодавство передбачає наявність або відсутність тих чи інших обмежень чи заборон. Але схема “відкритої та закритої інформації” не може до кінця розкрити особливості існуючих в інформаційних правовідносинах обмежень і заборон. Наприклад, схема не розрізняє інформації, яка містить державну таємницю і доступ до якої може бути наданий лише обмеженому колу осіб, та інформацію, яка може бути передана будь-яким зацікавленим особам за відповідну винагороду (ноу-хау), при чому це може бути як передача копії цієї інформації, так і повна передача усіх прав на подібну інформацію.

І відкрита інформація може бути закритою для певного кола осіб. Це наприклад, стосується заборони, відповідно до Положення “Про державне посвідчення на право розповсюдження і демонстрування фільмів”¹⁹⁰, Національною Радою України з питань телебачення і радіомовлення демонстрації по телебаченню фільмів з елементами насильства та еротики до 22.00. Крім того, в рамках такої класифікації абсолютно ігнорується система авторських прав та права власності на інформацію, за яких інформація може бути відкритою для доступу, але мати обмеження щодо розповсюдження або обробки.

Отже система правового регулювання обігу інформації складніша, ніж за режими доступу до інформації або правові режими інформаційних ресурсів, які є лише складовими цього регулювання. Основою класифікації можуть бути *методи правового регулювання*, які застосовують в регулюванні суспільного обігу того чи іншого виду інформації, – диспозитивний та імперативний.

За *диспозитивного методу* умови обігу інформації, її використання, розповсюдження, передачі прав на неї третім особам визначають-

¹⁹⁰ Про положення про державне посвідчення на право розповсюдження і демонстрування фільмів: Постанова Кабінету Міністрів України від 17 серпня 1998 р. № 1315.

ся або власником цієї інформації особисто, або на основі договору з іншими зацікавленими особами. Хоча є нормативно-правове регулювання обігу цієї інформації, в його межах передбачена відповідна свобода дії, наприклад, законодавство про авторські права, про право інтелектуальної власності; законодавство, що охороняє інформацію про особисте життя (адже ці дані також можуть бути оприлюднені за згодою цієї особи) та ін.

Існує специфічний обіг інформації, який регулюється *імперативним методом*, тобто чіткими законодавчими приписами і нормами поведінки, скасування яких за згодою сторін неможлива. Це стосується, зокрема, встановлених законом прямих обмежень державної, службової, лікарської, адвокатської таємниці, певних видів статистичної інформації, персональних та інших даних.

Застосування до обігу інформації диспозитивного регулювання не виключає одночасного існування певних імперативних заборон та обмежень, і навпаки.

Таким чином, два правових методи регулювання створюють три можливих види правового обігу інформації: *відкритий*, що регулюється диспозитивним методом (виключно цивільно-правовими нормами); *закритий*, що регулюється імперативним методом (адміністративно-правовими нормами); і *обмежений*, до якого застосовуються обидва види правового регулювання (Рис 6.1). До цих методів також долучається *вільний обіг інформації*, який безпосередньо правом не врегульований, але щодо якого можуть виникати охоронні правовідносини у разі порушення певних заборон чи обмежень. Причому інформація, змінюючи свою суспільну цінність, може переходити з одного виду обігу до іншого (зняття грифів “таємно”, або “для службового користування”, закінчення строку дії авторських прав тощо).

Інформація у відкритому обігу представлена всіма видами відкритої інформації, щодо доступу та розповсюдження якої немає жодних обмежень. Такою зокрема, є інформація: масова інформація, інформація про діяльність державних органів влади та органів місцевого самоврядування, правова, довідково-енциклопедична, соціологічна, екологічна, науково-технічна, відкрита статистична та інша інформація необмеженого доступу.

Основними характеристиками *відкритого обігу інформації* є:

- відносини щодо даного виду інформації врегульовано законодавством;

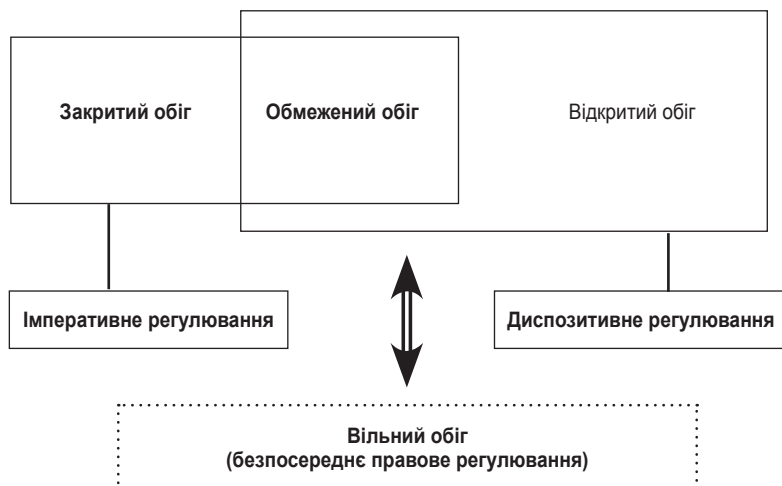


Рис 6.1. Види суспільного обігу інформації

- кожен суб'єкт інформаційних відносин має право на доступ до цієї інформації або безоплатно, або за певну плату;
- обмеження встановлює виключно власник та виключно для забезпечення власних інтересів;
- інформаційна продукція може вільно розповсюджуватися у будь-який спосіб.

До *інформації в закритому обігу*, як уже зазначалося, належить таємна і конфіденційна інформація, яка містить державну таємницю, конфіденційні дані про особу, конфіденційну інформацію, що перебуває у власності держави, комерційну таємницю, банківську таємницю, лікарську таємницю, адвокатську таємницю, таємницю слідства та судочинства, таємницю страхування і таємницю вчинення нотаріальних дій, іншу передбачену законом таємницю.

Закритий обіг інформації має такі основні характеристики:

- інформація вилучена з вільного обігу на підставі закону;
- законодавство надає інформації статусу конфіденційної або таємної;
- власник інформації здійснює заходи щодо її захисту;
- надання такої інформації третім особам або допуск до неї можливий лише у разі проведення певної процедури.

- отримання такої інформації пов'язане, як правило, із виконанням службових або професійних обов'язків.

Специфічною є *інформація в обмеженому обігу*, тобто така щодо якої не встановлено обмеженого режиму доступу, але разом з тим існують певні заборони або обмеження в її розповсюдженні, які встановлено зазвичай з метою захисту суспільної моралі та здоров'я і запобігання *негативному інформаційному впливу* на суспільство або окремі, найбільш вразливі його групи. Обмежений обіг інформації визначається насамперед заборонами щодо її поширення, як, наприклад, правила, встановлені нормами ст. 46 Закону України “Про інформацію”, дія яких поширюється на заклики до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання расової, національної, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини. До цієї ж групи належить заборонена в Україні порнографія. Іншу групу становить інформація, щодо розповсюдження якої законодавство встановлює обмеження. Останні можуть стосуватися аудиторії, на яку розповсюджується інформація (діти, неповнолітні), часу розповсюдження через електронні ЗМІ (денний, вечірній, нічний), місць розповсюдження (публічні місця, дитячі, освітні заклади) тощо. Такою, зокрема, є: інформація відео і друкована продукція що містить еротичу, елементи насильства та жорстокості, деякі види рекламної інформації тощо.

Обмежений обіг інформації має такі ознаки:

- інформація не є конфіденційною або таємною;
- законодавство встановлює певні обмеження щодо її розповсюдження;
- для отримання такої інформації суб'єкт має відповідати певним вимогам.

Нарешті, найбільш нерегульованою є *інформація у вільному обігу*, тобто така, яка через втрату суспільної цінності або її відсутність вільно розповсюджується в суспільстві. Ця інформація міститься в будь-яких документованих або оприлюднених відомостях, що не належать до попередніх трьох типів обігу інформації. Загальними характеристиками вільного обігу інформації є такі:

- відносини щодо цього виду інформації безпосередньо законодавством не врегульовані;

- розповсюдження інформації регулюється виключно морально-етичними нормами;
- охоронні правовідносини виникають лише у випадку, якщо розповсюдження такої інформації порушує права третіх осіб.

Важливою особливістю системи обігу інформації в суспільстві є те, що одна й та сама інформація з плином часу або через зміну певних обставин (втрата актуальності, закінчення строку режиму обмеження доступу або його порушення, закінчення строку дії авторських прав) може переміщуватися з одного виду обігу до іншого, відповідно змінюючи свій правовий режим.

6. 4. Обмеження щодо розповсюдження інформації

Обмеження доступу до інформації та обмеження щодо її розповсюдження, хоча і є винятками із загального принципу свободи інформації, різняться способами реалізації. Основні способи обмеження права на інформацію такі:

- установлення обов'язків щодо вжиття певних дій із захисту інформації з метою недопущення її несанкціонованого витоку, отримання та збирання;
- установлення зобов'язання утриматися від певних дій з метою запобігання розголошенню або розповсюдженню інформації.

Якщо до таємної і конфіденційної інформації застосовуються одночасно обидва способи обмеження, до забороненої або обмеженої до розповсюдження лише останній. Це стосується передбаченого багатьма міжнародно-правовими актами, зокрема Конвенцією про захист прав і основних свобод людини (ч. 2 ст. 10),¹⁹¹ обмежень для забезпечення територіальної цілісності або громадського порядку, для захисту здоров'я і моралі. В Україні існує система норм, різних законодавчих актів, які обмежують або забороняють розповсюдження інформації з певною метою. Усі заходи досягнення цієї мети можна поділити на три основні групи:

- норми, що забороняють або обмежують виготовлення інформаційної продукції;
- норми, що забороняють або обмежують ввезення інформаційної продукції на митну територію України;

¹⁹¹ Конвенція про захист прав і основних свобод людини 1950 року, Перший протокол та протоколи № 1, 4, 6, 7, 9, 10 та 11 до Конвенції (Рим, 4. XI. 1950) / . – № 5.

- норми, що встановлюють особливі правила здійснення інформаційної діяльності з розповсюдження певних видів інформації.

Закон України “Про захист суспільної моралі”¹⁹² (ст. 1) вводить поняття *державного регулювання і контролю обігу продукції, що негативно впливає на суспільну мораль*, яка представляє собою визначення законом і прийнятими на його основі нормативно-правовими актами порядку й умов обігу відповідної продукції та контроль за ним, виро-блення правових механізмів і встановлення прав та обов’язків органів державної влади, органів місцевого самоврядування, установ і організацій усіх форм власності по забезпеченню захисту суспільної моралі.

Основними напрямками державного регулювання обігу інформаційної продукції, що впливає на суспільну мораль, є:

- формування єдиної комплексної системи забезпечення захисту моральних засад і утвердження здорового способу життя у сфері інформаційної діяльності, освіти та культури;
- недопущення пропаганди в електронних та інших засобах масової інформації культу насильства, жорстокості, поширення порнографії;
- впровадження експертного оцінювання відео-, аудіо- та друкованої інформації й інформації на електронних носіях, розроблення механізмів і методик віднесення її до такої, що завдає шкоди суспільній моралі;
- підтримка національної культури, мистецтва, кінематографії, книговидавництва, поліпшення системи пропаганди кращих зразків світової літератури, культури та мистецтва;
- заборона демонстрації неліцензійної аудіо-, відеопродукції в усіх національних телерадіокомпаніях;
- встановлення контролю за обігом продукції, що становить загрозу суспільній моралі;
- приєднання до міжнародних договорів з питання захисту суспільної моралі.

Нормами ст. 2 зазначеного Закону встановлено такі обмеження і заборони щодо інформаційної продукції.

1) забороняється виробництво та обіг у будь-якій формі продукції порнографічного характеру;

2) забороняється виробництво та розповсюдження продукції, яка:

¹⁹² Про захист суспільної моралі: Закон України від 20 листопада 2003 р. №1296– IV// Відомості Верх. Ради України. – 2004. – №14. – Ст. 192.

- пропагує війну, національну та релігійну ворожнечу, зміну шляхом насильства конституційного ладу або територіальної цілісності України;
- пропагує фашизм і неофашизм;
- принижує або ображає націю чи особистість за національною ознакою;
- пропагує бузувірство, блюзнірство, неповагу до національних і релігійних святих;
- принижує особистість, є проявом знущання з приводу фізичних вад (каліцтва), з душевнохворих, літніх людей;
- пропагує невігластво, неповагу до батьків;
- пропагує наркоманію, токсикоманію, алкоголізм, тютюнопаління та інші шкідливі звички;

3) виробництво та обіг у будь-якій формі продукції еротичного характеру та продукції, що містить елементи насильства та жорстокості, дозволяються виключно за умови дотримання обмежень, установлених законодавством.

Зазначені обмеження передбачають розповсюдження продукції еротичного характеру та продукції, що містить елементи насильства й жорстокості, у спеціально відведених для цього місцях, визначених цим Законом, та у спосіб, установлений органами державної влади й органами місцевого самоврядування в межах своєї компетенції, запровадження ліцензування відповідних видів інформаційної діяльності.

Основні функції державного регулювання і контролю обігу продукції, що негативно впливає на суспільну мораль, покладено на Національну експертну комісію з питань захисту суспільної моралі, яка є постійнодіючим державним експертним і контролюючим органом¹⁹³.

Основні завдання цієї Комісії такі:

- проведення експертизи продукції, видовищних заходів сексуального чи еротичного характеру та продукції, що містить елементи або пропаганду культу насильства, жорстокості, порнографії;
- проведення аналізу процесів і тенденцій у сфері захисту суспільної моралі, розроблення для органів державної влади та органів місцевого самоврядування рекомендацій з їх правового регулювання;

¹⁹³ Про Національну експертну комісію України з питань захисту суспільної моралі: Постанова Кабінету Міністрів України від 17 листопада 2004 р. № 1550.

- здійснення контролю за дотриманням законодавства у сфері захисту суспільної моралі.

Комісія формується з провідних діячів культури, мистецтв, науки і освіти, психіатрів, сексопатологів, фахівців у галузі інформації та інших осіб за рекомендаціями юридичних осіб, у яких вони працюють.

Персональний склад Комісії затверджує Кабінет Міністрів України за поданням її Голови. Строк повноважень членів Комісії – 5 років.

Загальні правила, встановлені Законом України “Про захист суспільної моралі”, додатково конкретизуються в законодавчих актах, що регулюють окремі напрями інформаційної діяльності.

Так, Закон України “Про видавничу справу”¹⁹⁴ (ст. 28) передбачає, що діяльність у видавничій справі не може бути використана для закликів, спрямованих на ліквідацію незалежності України, зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності держави, підрив її безпеки, незаконне захоплення державної влади, пропаганду війни, насильства, розпалювання міжетнічної, расової, релігійної ворожнечі, посягання на права і свободи людини, здоров’я населення. З цією метою, зокрема, забороняється:

- виготовляти чи розповсюджувати продукцію, яка містить інформацію, віднесена до недобросовісної реклами, або рекламувати товари, послуги, які можуть завдати шкоди громадянам, підприємствам, установам, організаціям або державі;
- виготовляти чи розповсюджувати видавничу продукцію pornографічного характеру і таку, що пропагує культ насильства і жорстокості;
- виготовляти чи розповсюджувати видавничу продукцію, що проповідує релігійні віровчення, які загрожують життю, здоров’ю, моралі громадян, порушують їх права і свободи або закликають до порушення громадського порядку.

Норми ст. 13 Основ законодавства України про культуру¹⁹⁵ забороняють розповсюдження творів аналогічного змісту.

Відповідні переліки видів інформаційної продукції, які теле-радіоорганізації не мають права розповсюджувати в своїх про-

¹⁹⁴ Про видавничу справу: Закон України від 5 червня 1997 р. № 318/97-ВР. // Відомості Верховної Ради України. – 1997. – № 32. – Ст. 206.

¹⁹⁵ Основи законодавства України про культуру: Закон України від 14 лютого 1992 р. № 2117-XII // Відомості Верховної Ради України. – 1992. – № 21. – Ст. 294.

грамах, визначені нормами ч. 2 ст. 2. Закону “Про телебачення і радіомовлення”¹⁹⁶.

Регулювання питань захисту моральності та інформаційної безпеки суспільства в галузі виробництва, розповсюдження, зберігання і демонстрування кіно та відеопродукції здійснюється на основі Закону “Про кінематографію”¹⁹⁷.

Ще одна група правових норм спрямована на *недопущення ввезення забороненої до розповсюдження інформаційної продукції* на територію України або вивезення її з цієї території. Так, згідно із Законом “Про порядок ввезення (пересилання) в Україну, митного оформлення й оподаткування особистих речей, товарів та транспортних засобів, що ввозяться (пересилаються) громадянами на митну територію України”¹⁹⁸ (ст. 9), не підлягають пропуску через митний кордон України: літературні та художні твори, поліграфічна та інша друкована продукція, кіно-, фото-, аудіо- та відеоматеріали, що пропагують війну, жорстокість, порнографію, расову, етнічну або релігійну ворожнечу, закликають до насильницького повалення конституційного ладу в Україні.

Окремою сферою обмежень щодо розповсюдження інформаційної продукції є комерційна реклама. Так, ст. 7 Закону України “Про рекламу” визначає, що “основними принципами рекламної діяльності є: законність, точність, достовірність, використання державної та інших мов відповідно до законодавства України, використання форм та засобів, які не завдають споживачеві реклами моральної, фізичної або психічної шкоди”¹⁹⁹. Крім того, цей Закон установлює низку загальних обмежень в рекламній діяльності, серед яких заборони:

- поширювати інформацію щодо продукції, виробництво або реалізацію якої заборонено законодавством України;
- вмішувати твердження, які є дискримінаційними за ознаками походження, соціального і майнового стану, расової та націо-

¹⁹⁶ Про телебачення і радіомовлення: Закон України від 21 грудня 1993 р. № 3759-XII // Відомості Верховної Ради України. – 1994. – № 10. – Ст. 43. (В редакції закону від 11. 05. 2000 № 1709-III)

¹⁹⁷ Про кінематографію: Закон України від 13 січня 1998 р. № 9/98-ВР // Відомості Верховної Ради України. – 1998. – № 22. – Ст. 114.

¹⁹⁸ Про порядок ввезення (пересилання) в Україну, митного оформлення й оподаткування особистих речей, товарів та транспортних засобів, що ввозяться (пересилаються) громадянами на митну територію України: Закон України від 13 вересня 2001 р. № 2681-III // Відомості Верховної Ради України. – 2002. – № 1. – Ст. 2

¹⁹⁹ Про рекламу: Закон України від 3 липня 1996 року № 270/96-ВР // Відомості Верховної Ради України. – 1996. – № 39. – Ст. 181.

нальної належності, статі, освіти, ставлення до релігії, за мовними ознаками, за родом і характером занять, місцем проживання, за інших обставин або такі, що дискредитують продукцію інших осіб;

- подавати відомості або закликати до дій, які можуть спричинити порушення законодавства, завдають чи можуть завдати шкоди здоров'ю або життю людей та навколишньому природному середовищу, а також спонукають до нехтування засобами безпеки;
- використовувати засоби і технології, які безпосередньо діють на підсвідомість споживача;
- наводити твердження, що дискримінують осіб, які не користуються продукцією, що рекламується.

Інформаційно-психологічну безпеку особи захищає також норма ч. 8 ст. 20 Закону України “Про рекламу”, якою встановлено заборону реклами “лікувальних сеансів, інших аналогічних заходів з використанням гіпнозу та інших методів психічного або біоенергетичного впливу без дозволу Міністерства охорони здоров'я України”.

Законодавець приділяє також увагу захисту неповнолітніх від негативного впливу рекламної інформації. Така увага зумовлена підвищеною вразливістю, недостатнім життєвим досвідом цієї соціальної групи, внаслідок чого її представники дуже часто наражаються на вплив сторонніх осіб. Так, у рекламі, розрахованій на неповнолітніх (ст. 19 Закону “Про рекламу”), забороняється використовувати інформацію, яка може підірвати авторитет дорослих або дискредитувати довіру неповнолітніх до них; використовувати легковірність чи брак досвіду у неповнолітніх; використовувати справжню або іграшкову зброю. Крім того, така реклама не повинна містити тверджень або зображень неповнолітніх у небезпечних ситуаціях чи за обставин, що у разі їх імітації можуть завдати шкоди неповнолітнім або іншим особам, а також інформації, здатної викликати зневажливе ставлення неповнолітніх до небезпечних для здоров'я і життя ситуацій.

Додаткові обмеження визначено щодо телевізійної реклами відповідно до ст. 31 Закону “Про телебачення і радіомовлення”²⁰⁰.

Забороняється переривати з метою розміщення реклами трансляції сесій Верховної Ради України, Верховної Ради Автономної Респуб-

²⁰⁰ Про телебачення і радіомовлення: Закон України 21 грудня 1993 року № 3759-XII // Відомості Верховної Ради. – 1994. – № 10. – Ст. 43. (В ред. закону від 11. 05. 2000 № 1709-III)

бліки Крим, офіційних державних заходів і церемоній, виступів Президента України, Голови Верховної Ради України, Прем'єр-Містра України, Голови Конституційного Суду України, народних депутатів України, членів Уряду України.

Для молодшого покоління захист від негативного інформаційного впливу визначено, що реклама не повинна містити в тексті і зображенні того, що може завдати духовної, моральної або психічної шкоди молоді і дітям, а реклама в передачах, розрахованих на дитячу (до 14 років) аудиторію, взагалі забороняється.

Разом з тим у демократичному суспільстві необхідний пошук відповідного балансу між питаннями захисту моральності та правом на інформацію. І в цьому разі випадку на перше місце потрібно ставити *право кожної дієздатної людини самостійно вирішувати питання про відповідність її моральним принципам конкретної інформації*. І головним стандартом у цій сфері є вимоги щодо *обов'язкового попередження* про зміст інформаційного продукту та обмеження доступу до такого продукту неповнолітніх. В інших випадках застосування імперативних обмежень певною мірою починає межувати з цензурою та порушенням права на доступ до інформації.

Ще одним важливим аспектом проблеми, який, на жаль, все ще залишається поза увагою законодавця, є необхідність встановлення нормативно-правового регулювання пропаганди вчень та релігійної практики релігійних культів тоталітарного характеру. Проте, за даними досліджень²⁰¹, пропаганда нових релігійних учень та релігійної практики, що включає елементи нейрон-лінгвістичного програмування людини, набуває дедалі більшого поширення, в тому числі з використанням електронних ЗМІ.

²⁰¹ Чинники ескалації загроз інформаційній безпеці України // Національна безпека і оборона. – 2001. – № 1. – С 39.

ОСОБЛИВА ЧАСТИНА

РОЗДІЛ II ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ

ГЛАВА 7 ДЕРЖАВНА ТАЄМНИЦЯ

Поняття і правовий режим державної таємниці. Державні експерти з питань таємниць. Порядок засекречування інформації. ЗВДТ. Класифікація видів секретної інформації. Міжнародні передачі таємної інформації.

7. 1. Поняття і правовий режим державної таємниці.

Найбільш важливою і, відповідно, максимально захищеною вважається інформація, оголошена державною таємницею. Основним нормативно-правовим актом, що визначає режим державної таємниці, є Закон України “Про державну таємницю”²⁰². Він регулює суспільні відносини, що виникають з приводу віднесення певних відомостей до державної таємниці, їх розсекреченням та захист в інтересах національної безпеки України. Зокрема, цей Закон визначає:

- компетенцію органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці;
- здійснення права власності на секретну інформацію та її матеріальні носії;

²⁰² Про державну таємницю: Закон України від 21 січня 1994 року № 3855-XII // Відомості Верховної Ради. – 1994. – № 16. – Ст. 93. (В редакції Закону № 1079-XIV від 21. 09. 99)

- порядок віднесення інформації до державної таємниці;
- порядок засекречення і розсекречення матеріальних носіїв інформації;
- порядок охорони державної таємниці.

Згідно зі ст. 1 Закону “Про державну таємницю”, *державна таємниця (секретна інформація) є видом таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою.*

Отже, основними ознаками секретної інформації є:

- належність конкретних відомостей до визначених законодавством про державну таємницю сфер;
- наявність потенційної загрози національній безпеці у випадку розголошення цих відомостей;
- засекречування інформації відповідно до встановленої законодавством процедури;
- застосування державою заходів щодо охорони такої інформації.

Основною підставою класифікації секретної інформації є *ступінь секретності*. Ця категорія характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою. Законодавством передбачено три ступені секретності для інформації, що становить державну таємницю: “особливої важливості”, “цілком таємно”, “таємно”.

Зі ступенем секретності безпосередньо пов’язаний і максимальний строк дії режиму секретності інформації. Він не може перевищувати для інформації із ступенем секретності “особливої важливості” – 30 років, для інформації “цілком таємно” – 10 років, для інформації “таємно” – 5 років. У деяких випадках Президент України може встановлювати більш тривалі строки дії рішень про віднесення інформації до державної таємниці.

При встановленні режиму секретності інформації, що становить державну таємницю, слід виділити дві основні процедури: віднесення інформації до державної таємниці та засекречування матеріальних носіїв інформації.

Віднесення інформації до державної таємниці – це процедура ухвалення (державним експертом з питань таємниць) 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 нього.

Процедура віднесення інформації до державної таємниці стосується не конкретних відомостей або документів, а саме *категорій* відомостей. Тобто передбачає визначення певного змісту інформації, наявність якого зумовлює необхідність обмеження доступу до конкретної інформації чи документів.

Засекречування матеріальних носіїв інформації означає введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації.

Засекречування матеріальних носіїв інформації здійснюється на підставі рішення щодо віднесення інформації до державної таємниці. Рішення про засекречування матеріальних носіїв інформації ухвалюється у випадку належності інформації, що зафіксована на них, одній з категорій інформації, віднесеної до державної таємниці.

Охорона державної таємниці передбачає впровадження комплексу організаційно-правових заходів, до яких, зокрема, належать:

- єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;
- дозвільний порядок провадження діяльності, пов'язаної з державною таємницею;
- обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом секретної інформації;
- обмеження щодо доступу до державної таємниці іноземців, осіб без громадянства та іноземних юридичних осіб;
- режим секретності органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій, що проводять діяльність, пов'язану з державною таємницею;
- спеціальний порядок допуску та доступу громадян до державної таємниці;
- технічний і криптографічний захист секретної інформації.

Слід зазначити, що віднесення інформації до державної таємниці не виключає регулювання суспільних відносин щодо даної інформації нормами, що визначають право власності на інформацію, авторські права тощо. Згідно зі ст. 6 Закону України “Про державну таємницю”, власник секретної інформації або її матеріальних носіїв здійснює своє право власності з урахуванням обмежень, установлених в інтересах національної безпеки України відповідно до цього Закону.

У випадку, якщо обмеження права власності на секретну інформацію або її матеріальні носії завдають шкоди їх власнику, відшкодування здійснюється за рахунок держави у порядку та розмірах, що визначаються у договорі між власником такої інформації або її матеріальних носіїв і компетентним органом державної влади. Подібним договором також визначаються:

- порядок та умови охорони державної таємниці, включаючи режим секретності під час користування і розпорядження секретною інформацією та її матеріальними носіями;
- обумовлюється згода власника цієї інформації та її матеріальних носіїв на здійснення права власності з урахуванням обмежень, встановлених відповідно до Закону;
- взяття власником на себе зобов’язання щодо збереження державної таємниці та ознайомлення його з мірою відповідальності за порушення законодавства про державну таємницю.

У випадку відмови власника засекреченої інформації від укладення договору чи його порушення за рішенням суду відповідна інформація або її матеріальні носії можуть бути вилучені у власність держави за умови попереднього і повного відшкодування власникові їх вартості.

Законодавством визначено перелік інформації що не може бути засекречена. Так, за ст. 8 Закону України “Про державну таємницю” не належить до державної таємниці інформація:

- про стан довкілля, про якість харчових продуктів і предметів побуту;
- про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;
- про стан здоров’я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне

забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

- про факти порушень прав і свобод людини і громадянина;
- про незаконні дії органів державної влади, органів місцевого самоврядування та їх посадових осіб;
- інша інформація, яка відповідно до законів та міжнародних договорів, згода на обов’язковість яких надана Верховною Радою України, не може бути засекречена.

Процес надання фізичним особам права на отримання та використання інформації передбачає проведення певної, визначеної законодавством процедури та за умови додержання особою певних вимог. Ця процедура складається з двох основних етапів, першим із яких є надання *допуску до державної таємниці*, тобто *оформлення права громадянина на доступ до секретної інформації*. Слід уточнити використання в цьому визначенні терміна *громадянин*, адже за загальним правилом допуск до державної таємниці може надаватися лише дієздатним громадянам України віком від 18 років, які потребують його за умовами своєї службової, виробничої, наукової чи науково-дослідної діяльності або навчання.

Форми допуску до державної таємниці встановлюються залежно від ступеня секретності інформації. Законодавство передбачає три форми такого допуску: *форма 1* – для роботи із секретною інформацією, що має ступені секретності “особливої важливості”, “цілком таємно” і “таємно”, яка має термін дії 5 років; *форма 2* – для ступенів секретності “цілком таємно” і “таємно” з терміном дії 10 років; *форма 3* – для ступеня секретності “таємно” з терміном дії 15 років.

Згідно зі ст. 22 Закону України “Про державну таємницю” надання допуску громадян до державної таємниці передбачає:

- визначення необхідності роботи громадянина із секретною інформацією;
- перевірку громадянина у зв’язку з допуском до державної таємниці;
- взяття громадянином на себе письмового зобов’язання щодо збереження державної таємниці, яка буде йому довірена;
- одержання у письмовій формі згоди громадянина на передбачені законом обмеження прав у зв’язку з його допуском до державної таємниці;
- ознайомлення громадянина з мірою відповідальності за порушення законодавства про державну таємницю.

Безпосередньо перелік відомостей, які надає громадянин для оформлення допуску до державної таємниці, а також текст зобов'язання, яке він віддає, затверджено Наказом Голови СБУ “Про затвердження зобов'язання громадянина України у зв'язку з допуском до державної таємниці та анкети для оформлення допуску до державної таємниці”²⁰³.

Законодавством визначається вичепний перелік підстав, на яких громадянину може бути відмовлено у наданні допуску до державної таємниці. Згідно ст. 23 Закону України “Про державну таємницю”

Допуск до державної таємниці не надається у разі:

- відсутності у громадянина обґрунтованої необхідності в роботі із секретною інформацією;
- сприяння громадянином діяльності іноземної держави, іноземної організації чи їх представників, а також окремих іноземців чи осіб без громадянства, що завдає шкоди інтересам національної безпеки України, або участі громадянина в діяльності політичних партій та громадських організацій, діяльність яких заборонена у порядку, встановленому законом;
- відмови громадянина взяти на себе письмове зобов'язання щодо збереження державної таємниці, яка буде йому довірена, а також за відсутності його письмової згоди на передбачені законом обмеження прав у зв'язку з допуском до державної таємниці;
- наявності у громадянина судимості за тяжкі злочини, не погашеної чи не знятої у встановленому порядку;
- наявності у громадянина психічних захворювань, які можуть завдати шкоди охороні державної таємниці, відповідно до переліку, затвердженого Міністерством охорони здоров'я України і Службою безпеки України.

У наданні допуску до державної таємниці може бути відмовлено також у разі:

- повідомлення громадянином під час оформлення допуску недостовірних відомостей про себе;
- постійного проживання громадянина за кордоном або оформлення ним документів на виїзд для постійного проживання за кордоном;

²⁰³ Про затвердження зобов'язання громадянина України у зв'язку з допуском до державної таємниці та анкети для оформлення допуску до державної таємниці: Наказ Служби безпеки України № 190 від 18 червня 2001 р.

- невиконання громадянином обов'язків щодо збереження державної таємниці, яка йому довірена або довірялася раніше.

Окремою процедурою є надання допуску до державної таємниці керівникові органу державної влади, органу місцевого самоврядування, підприємства, установи, організації, допуск до державної таємниці якого передбачений його службовими обов'язками. В таких випадках допуск до державної таємниці надається наказом чи письмовим розпорядженням посадової особи, що призначає його на посаду.

За наявності у громадянина відповідним чином оформленого допуску до державної таємниці та відповідної потреби або у зв'язку з виконанням службових обов'язків ухвалюється рішення про надання доступу до державної таємниці.

Рішення про *доступ до державної таємниці* передбачає надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею.

Існує також механізм надання доступу до державної таємниці за посадою, що її займає особа. Так, доступ до державної таємниці усіх ступенів секретності надається після взяття ними письмового зобов'язання щодо збереження державної таємниці Президентом України, Голові Верховної Ради України, Прем'єр-Міністру України, Голові Верховного Суду України, Голові Конституційного Суду України, Генеральному прокурору України, Голові Служби безпеки України, народним депутатам України.

7. 2. Державні експерти з питань таємниць

Проведення процедури віднесення інформації до державної таємниці належить до компетенції *державних експертів з питань таємниць*. Правовий статус і повноваження державного експерта з питань таємниць визначаються нормами ст. 9 Закону України “Про державну таємницю”. При виконанні покладених на нього завдань державний експерт з питань таємниць, зокрема:

- приймає щодо віднесення інформації до державної таємниці зміни ступеня секретності цієї інформації та її розсекречування;
- дає висновок про шкоду національній безпеці України у разі розголошення конкретної секретної інформації;

- затверджує висновки щодо обізнаності з державною таємницею громадян, які мають чи мали допуск до державної таємниці;
- контролює обґрунтованість і правильність надання грифів секретності матеріальним носіям інформації, що становить державну таємницю.

Функції державного експерта з питань таємниць, за законодавством, виконують визначені посадові особи органів державної влади, підприємств, установ та організацій.

У Верховній Раді України функції державного експерта з питань таємниці виконує Голова Верховної Ради України.

В інших державних органах, Національній академії наук України, на підприємствах, в установах і організаціях посадові особи, що виконують функції державного експерта з питань таємниць, визначаються Президентом України за поданням Служби безпеки України на підставі пропозицій керівників відповідних державних органів, Національної академії наук України, підприємств, установ і організацій. Перелік цих посадових осіб визначається Указом Президента України “Про Перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць”²⁰⁴.

Законодавством передбачена можливість колегіального вирішення питань, пов’язаних із віднесенням інформації до державної таємниці, та засекречування відповідних матеріальних носіїв інформації. В цьому випадку державними експертами з питань таємниць, а також керівниками підприємств, установ та організацій можуть *створюватися експертні комісії з питань державної таємниці*²⁰⁵.

Можливі два типи експертних комісій: що створюються державними експертами з питань таємниць і такі, що створюються на підприємствах, в установах і організаціях.

Основним завданням експертних комісій, *які створюються державними експертами з питань таємниць*, є розгляд матеріалів та підготовка пропозицій про:

- віднесення інформації до державної таємниці, продовження терміну дії рішення про віднесення інформації до державної таємниці та скасування рішення про віднесення інформації до державної таємниці;

²⁰⁴ Про Перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць: Указ Президента України від 29 травня 2006 р. № 452/2006.

²⁰⁵ Про затвердження Положення про експертні комісії з питань державної таємниці: Наказ Служби безпеки України від 14 грудня 2004 р. № 696.

- визначення та зміну ступеня секретності інформації, віднесеної до державної таємниці.

Основними завданнями експертних комісій, які створюються на підприємствах, в установах і організаціях, є:

- підготовка пропозицій про віднесення інформації до державної таємниці,
- підготовка проектів рішень про зміну чи скасування грифів секретності, наданих матеріальним носіям секретної інформації;
- проведення експертного оцінювання документів, інших матеріальних носіїв інформації, які плануються для передачі іноземним делегаціям, групам чи окремим іноземцям;
- проведення експертної оцінки матеріалів, які готуються для публікації матеріалів у друкованих виданнях, передачі на телебаченні та радіо,

Персональний склад експертних комісій з питань державних таємниць визначається керівниками органів державної влади, підприємств, установ та організацій.

Основною формою роботи експертних комісій є засідання, рішення комісії оформлюються відповідним протоколом.

7. 3. Порядок засекречування інформації.

Єдиною підставою для встановлення, зміни або скасування режиму секретності інформації є рішення державного експерта з питань таємниць. Законодавство визначає необхідність додержання певної процедури при прийнятті таких рішень, коло суб'єктів, що можуть ініціювати таку процедуру, строки її проведення та критерії, за якими це рішення повинно прийматися.

Ініціювати розгляд питання про віднесення інформації до державної таємниці державний експерт може або за його власною ініціативою, або за зверненням керівників відповідних органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій чи громадян.

Відповідне рішення про віднесення інформації до державної таємниці ухвалюється державним експертом з питань таємниць не пізніше одного місяця з дня одержання звернення відповідного органу державної влади, органу місцевого самоврядування, підприємства, установи, організації чи громадянина.

Згідно із законодавством, рішення про віднесення інформації до державної таємниці має бути мотивованим і прийматися виключно на підставах, передбачених ст. 8 Закону України “Про державну таємницю”.

Нормами ст. 11 Закону України “Про державну таємницю” визначено перелік обов’язкових положень, які повинні міститися в рішенні державного експерта з питань таємниць. Цим рішенням визначаються:

- інформація, яка має становити державну таємницю, та її відповідність категоріям і вимогам, передбаченим ст. 8 Закону “Про державну таємницю”;
- підстави віднесення інформації до державної таємниці та обґрунтування шкоди національній безпеці України у разі її розголошення;
- ступінь секретності зазначеної інформації;
- обсяг фінансування заходів охорони такої інформації;
- орган державної влади, орган 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, що матимуть доступ до цієї інформації;
- строк, протягом якого діє рішення про віднесення інформації до державної таємниці.

Рішення державного експерта з питань таємниць про віднесення інформації до державної таємниці підлягає реєстрації Службою безпеки України у *Зводі відомостей, що становлять державну таємницю*. Після відповідної реєстрації рішення державного експерта з питань таємниць є обов’язковим для виконання на всій території України.

Законодавством передбачена також процедура зміни режиму секретності інформації, яка включає скасування рішення про віднесення інформації до державної таємниці (розсекречування), або прийняття рішення про підвищення або зниження ступеня секретності інформації. Ця процедура може бути ініційована:

- у випадку закінчення строку дії рішення про віднесення інформації до державної таємниці;
- державним експертом з питань таємниць за власною ініціативою;
- на підставі рішення суду.

У разі ухвалення державним експертом з питань таємниць висновку про скасування рішення про віднесення інформації до державної таємниці він є підставою для вилучення інформації зі Зводу відомостей, що становлять державну таємницю.

Як уже зазначалося, на підставі віднесення інформації до державної таємниці ухвалюється рішення про *засекречування матеріальних носіїв інформації*. Його здійснюють наданням відповідному документу, виробу чи іншому матеріальному носію інформації *грифу секретності* – реквізиту, що засвідчує ступінь секретності певної інформації.

Рішення про надання матеріальним носіям інформації грифу секретності проймають посадові особи, визначені керівником органу державної влади, органу місцевого самоврядування, підприємства, установи, організації, що провадить діяльність, пов'язану з державною таємницею.

Гриф секретності та інші відповідні реквізити наноситься або безпосередньо на матеріальний носій інформації, або за неможливості зазначається у супровідних документах. Реквізити кожного матеріального носія секретної інформації повинні містити:

- гриф секретності, який відповідає ступеню секретності інформації (“особливої важливості”, “цілком таємно”, “таємно”);
- дату і строк засекречування матеріального носія секретної інформації,
- підпис, його розшифрування та посаду особи, яка надала зазначений гриф;
- посилання на відповідний пункт (статтю) Зводу відомостей, що становлять державну таємницю.

У разі зміни ступеня секретності інформації або її розсекречування уповноважені посадові особи зобов'язані протягом шести місяців від дати ухвалення відповідного рішення забезпечити зміну грифу секретності на матеріальних носіях інформації або її розсекречування.

Закон України “Про державну таємницю” (ст. 17) передбачає право громадян та юридичних осіб на оскарження Рішення про засекречування матеріального носія інформації в порядку підлеглості вищому органу або посадовій особі чи до суду.

7. 4. Звід відомостей, що становлять державну таємницю. Класифікація видів секретної інформації.

Звід відомостей, що становлять державну таємницю, (ЗВДТ) формує і публікує в офіційних виданнях Служба безпеки України на підставі рішень державних експертів з питань таємниць. ЗВДТ, що становлять державну таємницю – єдина форма реєстрації цих відомостей в Україні²⁰⁶. З моменту опублікування ЗВДТ держава забезпечує захист і правову охорону відомостей, які зареєстровані в ньому. Реєстрація відомостей у ЗВДТ є підставою для надання документу, виробу чи іншому матеріальному носієві інформації, що містить ці відомості, грифу секретності, який відповідає ступеню секретності, установленому для них у ЗВДТ.

Зміни до ЗВДТ, що становлять державну таємницю, публікуються не пізніше трьох місяців від дня одержання відповідного рішення чи висновку.

Сам ЗВДТ є систематизованим переліком відомостей, що становлять державну таємницю. Цей перелік складається зі статей, пунктів та підпунктів. Відомості систематизуються в чотири великі групи (статті) відповідно до сфери державної діяльності:

- сфера оборони;
- сфера економіки;
- сфера зовнішніх відносин;
- сфера державної безпеки і охорони правопорядку.
- Відомості, що належать до кожної із цих груп, класифікуються на окремі пункти та підпункти за основними характеристиками:
- змісту відомостей, що становлять державну таємницю;
- ступеня секретності (“особливої важливості”, “цілком таємно”, “таємно”);
- строку дії рішення про віднесення інформації у роках (30 років, 10 років, 5 років).

Реєстрація відомостей у ЗВДТ є підставою для надання документу, виробу чи іншому матеріальному носію інформації, що містить ці відомості, грифу секретності, який відповідає ступеню секретності, встановленому для них у ЗВДТ. Самі записи в ЗВДТ не повинні містити державних секретів.

²⁰⁶ Про затвердження Зводу відомостей, що становлять державну таємницю: Наказ Служби Безпеки України від 12 серпня 2005 р. № 440.

Перелік відомостей, що становлять державну таємницю, у рамках визначених Законом “Про державну таємницю” та ЗВДТ чотирьох основних сфер, можна також умовно класифікувати за деякими напрямками та видами інформації. Так, у військовій сфері можна виділити інформацію, що стосується безпосередньо Збройних сил України, до якої, зокрема, віднесено відомості:

- про зміст оперативних планів і документів бойового управління директив, бойових наказів, донесень та зведень;
- про підготовку військ до виконання оперативних (бойових) завдань;
- про систему бойового чергування;
- про стратегічне розгортання та зміст мобілізаційних завдань, оперативно-мобілізаційних заходів;
- про зміст закритих навчальних програм у вищих військових навчальних закладах Збройних сил України.
- Іншу групу можна кваліфікувати як інформацію військово-технічного характеру. Це, зокрема відомості:
- про військові об’єкти, зразки озброєння і військової техніки, органи державної влади і режимні об’єкти, підприємства, установи та організації, що підлягають захисту від засобів технічних розвідок;
- про норми технічного захисту інформації, віднесеної до державної таємниці;
- про нові зразки озброєння та військової техніки, нові технології створення та модернізації зразків озброєння та військової техніки;
- про досягнення науки і техніки, які можуть бути використані для потреб оборони і мають принципове значення для розробки нових видів озброєння та військової техніки;
- про систему фізичного захисту ядерних установок, ядерних матеріалів.

Приділено також увагу захисту інформації, яка стосується заходів захисту населення в умовах можливих військових конфліктів. Так, у ЗВДТ включено інформацію:

- про управління системою Цивільної оборони України в умовах військового часу;
- про схеми та джерела водозабезпечення, заходи їх охорони;
- про особливо важливі та важливі об’єкти, які беруться під військову і воєнізовану пожежну охорону в умовах воєнного стану.

І, нарешті, до державної таємниці у військовій сфері віднесено низку відомостей географічно-топографічного характеру, які мають важливе значення для бойового застосування військ, зокрема:

- про результати роботи щодо створення й уточнення державної системи координат і геодезичних параметрів, розробку і застосування національних космічних топогеодезичних засобів для забезпечення Збройних сил України;
- геодезичні дані, топографічні і картографічні матеріали з певними характеристиками, оприлюднення яких можливе лише після узгодження відповідно до законодавства.

Наступною сферою класифікації відомостей, що становлять державну таємницю, є сфера економіки. Серед інформації економічного характеру, що її внесено до ЗВДТ, також можна виділити кілька основних груп.

По-перше, це інформація військово-економічного характеру, захист якої є одним із заходів забезпечення функціонування економіки України в умовах воєнного стану, матеріально-технічного забезпечення Збройних сил та підприємств оборонного призначення. Наприклад, до ЗВДТ внесено відомості, які характеризують:

- виробничі потужності мобілізаційного призначення галузей національної економіки щодо виробництва оборонної продукції;
- заходи для забезпечення сталості функціонування галузей економіки України в умовах воєнного стану;
- кількість, вартість, строки постачання озброєння і військової техніки у Збройних силах України та військових формуваннях;
- номенклатуру, кількість, строки постачання військових формувань основними видами пального і мастильних матеріалів, речового та медичного майна, продовольства тощо.

Як стратегічну охарактеризовано економічну інформацію, що розкриває характеристики забезпеченості економіки України стратегічними або критично-необхідними сировиною і матеріалами. У ЗВДТ це, наприклад, відомості:

- про розміри і розміщення стратегічних запасів та резервів нафти, газу і нафтопродуктів України;
- про балансові запаси корисних копалин у надрах та обсяги їх видобутку (виробництва) в Україні;
- про балансові запаси урану в надрах України;

- оперативно-статистичні дані митних органів про експортно-імпорتنі операції з окремими стратегічними видами сировини і продукції;
- про магістральні або внутрішньозонові лінії зв'язку, мереж зв'язку загального користування із зазначенням трас проходження через об'єкти зв'язку, що належать до мобілізаційних потужностей господарства України.

Нарешті, останню групу становлять відомості, захист яких здійснюється в інтересах забезпечення нормального функціонування кредитно-фінансової системи України. До цієї групи належать такі відомості:

- про номенклатуру та обсяги матеріальних цінностей державного резерву;
- про кількість надходження до Державного фонду дорогоцінних металів і дорогоцінного каміння України, про відпуск їх на потреби народного господарства за період від одного року і більше, про планові обсяги реалізації золота за вільноконвертовану валюту або кількість золота, яке видано на закупівлю за кордоном товарів, за період від одного року і більше;
- про розроблені монетним двором Національного банку України банкноти і монети України нових зразків;
- про засоби захисту від підробки банкнот, бланків державних цінних паперів і документів суворого обліку України (крім відомостей про загальновідомі засоби захисту);
- про технології виготовлення та застосування спеціальних складових захисних голографічних елементів, які створюються на замовлення органів державної влади, у тому числі для захисту від підробки банкнот, цінних паперів, документів суворого обліку.

У сфері зовнішніх відносин визначено два основних види інформації, що становить державну таємницю і підлягає охороні.

По-перше, це інформація, розголошення якої може завдати шкоди зовнішньополітичній діяльності України, в т. ч. відомості, що містяться в директивах, планах та вказівках делегаціям і посадовим особам, які представляють Україну, розголошення яких розкриває стратегію і тактику зовнішньої політики України.

По-друге, це інформація про деякі аспекти міждержавної військово-економічного співпраці, яка, згідно із законодавством України або її міжнародно-правовими зобов'язаннями, є таємною. Це, зо-

крема, стосується відомостей про номенклатуру, обсяги та фінансування операцій з експорту, імпорту озброєння, військової техніки, окремих стратегічних видів сировини і продукції, а також відомостей про військову, військово-технічну та науково-технічну співпрацю з іноземними державами тощо.

Ще однією сферою інформації, яка становить державну таємницю, що її виділяє національне законодавство, є сфера державної безпеки і охорони правопорядку. Серед переліку відповідних відомостей, наведених у ЗВДТ, також можна виокремити декілька характерних напрямів.

По-перше, це інформація про деякі аспекти негласної та правоохоронної діяльності, яка впроваджується правоохоронними органами та військовими підрозділами України, а також про особовий склад і підготовку відповідних підрозділів і осіб, що здійснюють подібну діяльність. Зокрема, це інформація:

- про зміст, плани, організацію і результати оперативно-розшукової та розвідувальної діяльності, її конкретні засоби, форми і методи;
- про отримані результати ведення агентурної та спеціальної розвідки, радіоелектронної розвідки, контролю безпеки інформації та зв'язку тощо;
- про штат, штатну розстановку, стан, зміст і організацію бойової і спеціальної підготовки особового складу Служби безпеки України, Головного управління розвідки Міністерства оборони України, Управління державної охорони.

Наступну групу становить інформація про заходи охорони різних режимних об'єктів, осіб та матеріальних цінностей, які взято під державну охорону. До неї, зокрема, належать відомості:

про технічні системи забезпечення діяльності, охорони, зв'язку, зміст заходів пропускового і внутрішньооб'єктового режиму об'єкта СБУ, Управління державної охорони та Прикордонних військ, на якому впроваджено особливий режим;

- про організацію, стан і способи охорони установ кримінально-виконавчої системи;
- про заходи охорони органів державної влади, осіб та об'єктів, щодо яких здійснюється державна охорона;
- про організацію та порядок забезпечення безпеки пересування територією України вищих посадових осіб України та урядових делегацій іноземних держав;

- про строки, маршрути та організацію охорони перевезення банкнот і монет та інших цінностей у системі Національного банку України.

До останньої групи можна віднести інформацію про безпосереднє здійснення заходів захисту інформації та державної таємниці. Це, зокрема, відомості:

- про забезпечення безпеки систем урядового та спеціального зв'язку, про зміст заходів щодо комплексного технічного захисту інформації у цих системах від технічних засобів розвідки;
- про організацію та фактичний стан охорони державної таємниці тощо.

Слід зазначити, що рівень таємності відомостей, внесених до ЗВДТ, залежить не тільки від їх змісту цих відомостей, а й від конкретного об'єкта, інформацію щодо якого ці відомості розкривають. Наприклад, відомості про зміст оперативних планів щодо Збройних сил України мають гриф “особливої важливості” і мають строк секретності 30 років, щодо корпусу – “цілком таємно” зі строком секретності 10 років, щодо дивізії – “таємно” зі строком секретності 5 років.

Деякі фахівці вважають за доцільне використання досвіду, коли в подібних нормативно-правових актах визначається коло державних органів, до компетенції яких входить розпорядження (передача, допуск) тим чи іншим видом відомостей, що становлять державну таємницю, як це, наприклад, робиться у сусідній Російській Федерації²⁰⁷. Це допомогло б упорядкувати процеси допуску до секретної інформації, визначати органи відповідальні за надання того чи іншого виду секретної інформації, та ін.

7. 5. Міжнародні передачі таємної інформації.

Окремим аспектом забезпечення режиму секретності інформації, що належить до державної таємниці, є встановлення особливих правил передачі такої інформації іншим державам.

Згідно зі ст. 32 Закону України “Про державну таємницю”, секретна інформація до скасування рішення про віднесення її до державної таємниці і матеріальні носії такої інформації до їх розсекречування можуть бути передані іноземній державі чи міжнародній організації

²⁰⁷ О перечне сведений, отнесенных к государственной тайне: Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203 // Собрание Законодательства РФ, 1995, № 49, ст. 4775 (В редакции Указа от 24. 01. 98 № 61).

лише на підставі міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, або письмового мотивованого розпорядження Президента України з урахуванням необхідності забезпечення національної безпеки України на підставі пропозицій Ради національної безпеки і оборони України.

Основною складністю при цьому є вирішення питань забезпечення режиму секретності інформації на території іншої держави. Як правило, практика знає два шляхи виконання такого завдання.

По-перше, іноді застосовується процедура, за допомогою якої визначають відповідність ступенів секретності інформації в різних державах, і відповідно інша держава забезпечує захист переданої їй секретної інформації за її національним законодавством режимами секретності. Наприклад, за ст. 3 Закону “Про державну таємницю”, передані Україні відомості, що становлять таємницю іноземної держави чи міжнародної організації, охороняються в порядку, передбаченому цим Законом.

По-друге, безпосередньо міжнародним договором можуть визначитися правовий режим обмеження доступу та особливі вимоги до захисту інформації з певним ступенем секретності. В такому разі держава, якій передано секретну інформацію, забезпечує її захист відповідно до режиму обмеження доступу, визначеного нормами міжнародного договору, які можуть відрізнятися від тих, що передбачені національним законодавством.

Слід зазначити, що в рамках міжнародних угод визначаються не лише особливі вимоги до забезпечення режимів секретності інформації, але можуть встановлюватися і особливі визначення та критерії віднесення інформації до таємної та цілі її захисту.

Так, згідно з угодою між Україною і Французькою Республікою (ст. 1)²⁰⁸, застосовуються терміни “таємна інформація та матеріали”, під якими розуміють інформацію та матеріали будь-якого характеру, яким був присвоєний ступінь секретності, зазначений у цій Угоді, і які в інтересах національної безпеки відповідно до національного законодавства сторін підлягають охороні від одного з таких випадків:

- компрометації, знищення, нецільового використання, крадіжки, розголошення або втрати таємної інформації та матеріалів;

²⁰⁸ Угода між Урядом України та Урядом Французької Республіки про взаємну охорону таємної інформації та матеріалів від 7 грудня 1999 року. (Схвалено і подано на ратифікацію Постановою Кабінету Міністрів № 468 від 06. 05. 2001).

- доступу до такої таємної інформації та матеріалів будь-якої особи, що не має допуску.

При цьому “таємна інформація” визначається як “будь-яка інформація, зміст якої є таємним, незалежно від форми, у якій вона подана, та способу її передачі”, що відповідає українському визначенню “секретна інформація”. Поняття “таємні матеріали”, визначені як “будь-які носії інформації, незалежно від їх виду, зокрема, будь-який документ або виріб, на/в яких таємна інформація записана чи розміщена, не порушуючи їх фізичних ознак”, фактично відповідає українському терміну “матеріальні носії інформації”.

А от відповідно до угоди між Україною і Німеччиною поняття таємної інформації розглядається в комплексі і визначається (ст. 1): “Таємною інформацією у розумінні цієї Угоди є факти, об’єкти або відомості незалежно від форми їх представлення, які в державних інтересах підлягають збереженню в таємниці. Зокрема, це інформація у будь-якій формі, а також будь-які документи, вироби, речовини або фізичні поля, на/в яких інформація міститься або може бути записана, і які в інтересах національної безпеки Сторін, згідно з їх чинним законодавством, підлягають захисту від несанкціонованого доступу і засекречені відповідним чином. Таємній інформації державним органом або за його розпорядженням надається ступінь секретності, що відповідає необхідному рівню захисту. Сюди також включається таємна інформація, створена організаціями сторін у рамках співробітництва та засекречена на основі чинного законодавства сторін та відповідно до критеріїв цієї Угоди.”²⁰⁹.

Ця ж угода між Україною та Німеччиною є прикладом одночасного застосування двох підходів до забезпечення відповідного режиму секретності інформації, що передається іншій державі. Так, згідно зі ст. 2 цієї Угоди, запроваджено порівняння режимів таємної інформації. Українському грифу “Цілком таємно” відповідає німецький гриф *GEHEIM*, а грифу “Таємно” – *VS-VERTRAULICH*. В Україні щодо отриманої з Німеччини, таємної інформації яка має гриф “*VS-NUR FÜR DEN DIENSTGEBRAUCH*” (*VS-NfD*), застосовується специфічний режим, визначений Додатком до цієї Угоди.

²⁰⁹ Угода між Кабінетом Міністрів України та Урядом Федеративної Республіки Німеччина про взаємний захист таємної інформації від 29 травня 1998 р. (Затверджено Постановою Кабінету Міністрів України № 1433 від 14. 09. 98).

Основна характеристика режиму секретності таємної інформації з грифом *VS-NfD* – надається доступ до неї тільки особам, для яких він необхідний (принцип: знання тільки тоді, коли воно необхідне). Зміст таємної інформації з грифом *VS-NfD* має зберігатися в таємниці. Ця інформація зберігається у замкнених приміщеннях, шафах або столах, може бути передана кур'єром або надіслана у запечатаній упаковці. Якщо така інформація обробляється або передається далі за допомогою інформаційної техніки, то обов'язково має бути зашифрованою. Фізичні та юридичні особи, яким передається така інформація, повинні бути ознайомлені з Додатком, що регулює правила поводження з цією інформацією.

З подальшим розширенням міжнародної співпраці України, зокрема у сферах оборони, боротьби зі злочинністю, військово-технічного співпраці, питання міжнародно-правового регулювання захисту таємної інформації ставатимуть ще актуальнішими.

ГЛАВА 8

КОНФІДЕНЦІЙНА ІНФОРМАЦІЯ

Конфіденційна інформація, що є власністю держави. Комерційна таємниця. Професійна таємниця. Банківська таємниця.

8. 1. Конфіденційна інформація, що є власністю держави

Основними загальними ознаками конфіденційної інформації, за ст. 30 Закону України “Про інформацію”, є неналежність її до державної або іншої визначеної законом таємниці та встановлення обмежень на доступ до такої інформації її власником або особою, що користується та розпоряджається такою інформацією на законних підставах. Відповідно, однією з основ класифікації різних видів конфіденційної інформації є саме форма власності на таку інформації. За цим критерієм можна виділити конфіденційну інформацію, що є власністю держави та комерційну таємницю.

Так, ч. 3 ст. 30 Закону України “Про інформацію” визначає, що: стосовно інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, з метою її збереження може бути відповідно до закону встановлено обмежений доступ – надано статус конфіденційної.

Порядок обліку, зберігання і використання документів та інших носіїв інформації, що містять зазначену інформацію, визначається Кабінетом Міністрів України.

Поняття “конфіденційна інформація, що знаходиться у власності держави”, охоплює широке коло відомостей, що збираються, обробляються, зберігаються в процесі діяльності органів державної влади та місцевого самоврядування, інших державних установ і організацій. Для визначення цього виду інформації використовують також терміни “*службова таємниця*” та, відповідно до грифу обмеження доступу, що надається її матеріальним носіям, – “*інформація для службового користування*” (ДСК).

Термін “службова таємниця” використовується у зв’язку з тим, що найбільше вид інформації використовують органи виконавчої вла-

ди та місцевого самоврядування, і доступ до її використання безпосередньо пов'язані з виконанням посадовими особами своїх службових обов'язків. В науковій літературі досить поширеним є таке визначення: “Службова таємниця – це конфіденційна інформація, що захищається законом і стала відома в державних органах та органах місцевого самоврядування тільки на законних підставах і у зв'язку виконанням їх представниками службових обов'язків, а також службова інформація про діяльність державних органів, доступ до якої обмежений законом”²¹⁰.

Основні ознаки цього виду конфіденційної інформації такі:

1) вона є власністю держави.
2) її використання, поширення і зберігання здійснюють, як правило, посадові особи, які є державними або муніципальними службовцями у зв'язку з виконанням своїх службових обов'язків відповідно до закону;

3) режим цієї інформації, який визначає: порядок її віднесення до службової таємниці та розсекречування, порядок захисту, зберігання, передачі та доступу до неї, встановлюється спеціальними нормативно-правовими актами.

Ч. 4 ст. 30 Закону України “Про інформацію” дає перелік відомостей, які *не можуть* бути віднесені до конфіденційної інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності. Цей перелік містить відомості про:

- стан довкілля, якість харчових продуктів і предметів побуту;
- аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, що сталися або можуть статися і загрожують безпеці громадян;
- стан здоров'я населення, його життєвий рівень, зокрема, харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;
- стан справ із правами і свободами людини та громадянина, а також факти їх порушень;
- незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

²¹⁰ Див. : Бачило І. Л. , Лопатин В. Н. , Федотов М. А. Информационное право. / Под. ред. акад. РАН Б. Н. Топорнина. – СПб. : Юрид. центр Пресс, 2001. – С. 554.

- іншу інформацію, доступ до якої відповідно до законів України та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути обмеженим.

Загальні вимоги до захисту службової таємниці визначено Законом України “Про державну службу”. Ст. 10 цього Закону серед обов'язків державного службовця, визначає зокрема, “збереження державної таємниці, інформації про громадян, що стала їм відома під час виконання обов'язків державної служби, а також іншої інформації, яка згідно з законодавством не підлягає розголошенню”²¹¹.

Положення Закону України “Про державну службу” розкриваються також у Загальних правилах поведінки державного службовця, (п. 20): “Державному службовцю забороняється розголошувати довірену йому державну таємницю, іншу інформацію з обмеженим доступом, установлену Законами України “Про інформацію” та “Про державну таємницю”, у тому числі й після залишення ним державної служби, а також використовувати таку інформацію для власного інтересу або інтересу інших осіб шляхом порад чи рекомендацій”²¹².

Аналогічну вимогу до “збереження державної таємниці, інформації про громадян, що стала їм відома у зв'язку з виконанням службових обов'язків, а також іншої інформації, яка згідно із законом не підлягає розголошенню” містять і норми ст. 8 Закону України “Про службу в органах місцевого самоврядування”, якою встановлено основні обов'язки посадових осіб органів місцевого самоврядування²¹³.

Основним нормативно-правовим актом, який регулює питання службової таємниці, є затверджена Постановою Кабінету Міністрів України “Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави”²¹⁴.

Відповідно до цієї інструкції органи державної влади розробляють і затверджують відомчі інструкції з питань обліку, зберігання і

²¹¹ Про державну службу: Закон України від 16 грудня 1993 року № 3723-ХІІ // Відомості Верховної Ради. – 1993. – № 52. – Ст. 490.

²¹² Про затвердження Загальних правил поведінки державного службовця: Наказ Голового управління державної служби України № 58 від 23 жовтня 2000 р.

²¹³ Про службу в органах місцевого самоврядування: Закон України від 7 червня 2001 року № 2493-ІІІ // Відомості Верховної Ради. – 2001. – № 33. – Ст. 175.

²¹⁴ Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави: Постанова Кабінету Міністрів України від 27 листопада 1998 р. № 1893.

використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави; та розробляють і вводять в дію переліки конфіденційної інформації, що є власністю держави.

За цією Інструкцією переліки відомостей, що містять конфіденційну інформацію і є власністю держави і яким надається гриф обмеження доступу “Для службового користування”, розробляють експертні комісії і затверджують міністерства²¹⁵, інші центральні органи виконавчої влади, Рада міністрів АРК, облдержадміністрації.

Експертні комісії створюють у центральних органах виконавчої влади, Раді міністрів АРК та облдержадміністраціях. Їх особовий склад затверджується керівниками відповідних органів виконавчої влади. У складі експертних комісій працюють представники режимно-секретного та інших структурних підрозділів із найбільш кваліфікованих фахівців.

При вирішенні питань визначення переліків відомостей, яким надається гриф “Для службового користування” використовуються визначені Кабінетом Міністрів “Орієнтовні критерії віднесення інформації до конфіденційної” (Додаток 13 до Постанови КМУ №1893). Згідно з цими критеріями інформація, що міститься в переліках відомостей, що містять конфіденційну інформацію, котра є власністю держави, повинна відповідати таким вимогам:

- 1) створюватися коштом державного бюджету або перебувати у володінні, користуванні чи розпорядженні організації;
- 2) використовуватися з метою забезпечення національних інтересів держави;
- 3) не належати до державної таємниці;
- 4) унаслідок розголошення такої інформації можливе:
 - порушення конституційних прав і свобод людини та громадянина;
 - настання негативних наслідків у внутрішньополітичній, зовнішньополітичній, економічній, військовій, соціальній, гуманітарній, науково-технологічній, екологічній, інформаційній сферах та у сферах державної безпеки і безпеки державного кордону;
 - створення перешкод у роботі державних органів.

²¹⁵ Див. напр.: Про затвердження Переліку конфіденційної інформації: Наказ Міністерства палива та енергетики України від 15 липня 2006 р. № 288.

Захист конфіденційної інформації та її матеріальних носіїв, яким надано гриф “Для службового користування”, здійснюється за допомогою комплексу організаційних та правових заходів. Так, режим обмеження доступу до такої інформації передбачає запровадження особливих порядків реєстрації, зберігання та передачі відповідних документів.

Реєстрації підлягають усі вхідні, вихідні та внутрішні документи з грифом “Для службового користування”. Вони обліковуються за кількістю сторінок, а видання (книги, журнали, брошури) – за кількістю примірників.

Зберігаються документи із грифом “Для службового користування” виключно у службових приміщеннях і бібліотеках у шафах (сховищах), які надійно замикаються та опечатуються.

Передача конфіденційної інформації, що є власністю держави, каналами зв’язку здійснюється лише з використанням засобів технічного та (або) криптографічного її захисту.

Законодавство також визначає перелік вимог до працівників організацій, які мають справу з документами із грифом “Для службового користування”. Такі працівники перед допуском до роботи з документами з грифом “Для службового користування” обов’язково мають ознайомитися під розписку із зазначеною Інструкцією, що затверджена Кабінетом Міністрів України, та відповідними відомчими інструкціями.

Відповідно до системи обмежень у використанні та розповсюдженні інформації, що міститься в документах з грифом “Для службового користування”, працівникам забороняється:

- повідомляти усно або письмово будь-кому відомості, що містяться у цих документах, якщо це не викликано службовою потребою;
- користуватися відомостями з документів з грифом “Для службового користування” для відкритих виступів або опублікування у засобах масової інформації;
- експонувати такі документи в громадських місцях.

Контроль за дотриманням режиму конфіденційної інформації, що перебуває у власності держави, покладено на Службу безпеки України²¹⁶. Цей контроль вона здійснює проводячи планові та позапланові

²¹⁶ Про затвердження Інструкції про порядок здійснення Службою безпеки України контролю за обігом документів, які містять конфіденційну інформацію, що є власністю держави: Наказ Служби безпеки України 17 липня 2006 р. № 550.

перевірки. Крім того, для вивчення фактичного стану усунення порушень і недоліків, які було виявлено попередніми перевітками, та виконання рекомендацій, наданих за результатами цих перевірок, проводяться контрольні перевірки, проведення цих перевірок віднесено до компетенції Управління охорони державної таємниці СБУ, яке здійснює перевірки в центральних органах виконавчої влади, м. Києві та Київській області, та підрозділів охорони державної таємниці (ПОДТ) регіональних управлінь СБУ, які здійснюють відповідні перевірки в органах влади, підприємствах, установах та організаціях, розташованих в Автономній Республіці Крим, м. Севастополі та областях.

У провденні перевірок також беруть участь оперативні підрозділи СБУ, у сфері контррозвідального забезпечення яких перебувають організації, які підлягають перевірці. Ці оперативні підрозділи, отримавши повідомлення про заплановану перевірку, не пізніше ніж за два тижні до початку перевірки письмово інформують ПОДТ про додержання організаціями, що перевірятимуться, законодавства у сфері охорони конфіденційної інформації, що є власністю держави, можливі передумови до розголошення цієї інформації та/або втрати її матеріальних носіїв, надають пропозиції щодо порядку проведення та напрямів перевірки, а також уключення до складу комісії співробітників цих підрозділів.

Під час проведення перевірок обігу документів, які містять конфіденційну інформацію, що є власністю держави, предметами контролю є:

- акти попередніх перевірок, матеріали службових розслідувань за фактами розголошення конфіденційної інформації, що є власністю держави, втрати її матеріальних носіїв (були місце такі факти), стан виконання викладених у них рекомендацій;
- умови зберігання документів та роботи з ними, включаючи порядок складання, оформлення, друкування, обліку, приймання, розсилання (відправлення), розмноження, використання, знищення, передачі документів на архівне зберігання;
- особливості оброблення, зберігання, друкування документів з використанням автоматизованих систем;
- порядок передачі документів за кордон;
- фактична наявність матеріальних носіїв конфіденційної інформації, що є власністю держави;
- порядок охорони конфіденційної інформації, що є власністю

держави, під час прийому іноземних делегацій, груп та окремих іноземців.

При створенні відомих переліків конфіденційної інформації, що перебуває у власності держави, можливе запровадження додаткових класифікацій такої інформації залежно від порядку надання доступу до неї та особливостей застосування заходів щодо її охорони.

Наприклад, згідно з наказом Держмитслужби України “Про електронну інформацію в митній системі України”²¹⁷ (п. 2), було встановлено, що будь-яка митна електронна інформація, яка обробляється засобами електронної обчислювальної техніки митної установи, є інформацією з обмеженим доступом. Цю інформацію з обмеженим доступом за ступенем конфіденційності поділяють на три категорії:

А. Інформація та інформаційно-програмне забезпечення, яке не несе в собі даних, що безпосередньо визначають або зумовлюють характер митної діяльності (технічні дані обладнання, документи про роботу з персоналом, загальносистемне програмне забезпечення для передачі, оброблення та збереження митної інформації, прикладне програмне забезпечення тощо).

Б. Технологічна інформація діяльності митних органів (зміст митних декларацій, провізних відомостей, протоколів порушень митних правил та контрабанди, гарантійних листів тощо) та нормативно-довідкова інформація (кадри, бухгалтерія тощо).

В. Нормативно-правова інформація суто службового призначення, інформація про зовнішньоекономічну діяльність, інформація щодо групових статистичних баз даних.

Відповідно встановлено і порядок доступу до цієї інформації, згідно з яким (п. 4. 2.):

Інформація категорії “А” готується і використовується будь-яким працівником митної установи. Згідно з вимогами авторського права та умовами дотримання права власності на програмне забезпечення, яке виробляється власними силами або купується в інших установах, вона не може розповсюджуватись без відповідного дозволу власника інформації.

Інформація категорії “Б” готується працівником митної установи за розпорядженням керівництва. За розпорядженням або дозво-

²¹⁷ Про електронну інформацію в митній системі України: Наказ Державного Митного Комітету від 08 лютого 1996 р. № 48.

лом керівника митної установи інформація цієї категорії може передаватись для використання іншим митним установам України. Передача інформації категорії “Б” відомствам та установам, що не входять в митну систему України, в кожному окремому випадку погоджується з керівництвом Державної митної служби України.

Інформація категорії “В” готується та використовується виключно персоналом, який має спеціальний дозвіл. Ця інформація повинна зберігатись в закодованому вигляді, до неї мають вживатися заходи організаційного та програмно-апаратного захисту. Вона не може бути розповсюджена без письмового дозволу керівництва Державної митної служби України.

Разом з тим законодавство передбачає відповідальність (насамперед дисциплінарну та адміністративну) не лише за порушення правил обігу документів, які містять конфіденційну інформацію, що є власністю держави, але й за незаконне засекречування інформації та надання їй грифу обмеження доступу.

8. 2. Комерційна таємниця

Комерційна таємниця є одним із видів конфіденційної інформації. Як і щодо службові таємниці, застосування обмежень доступу до цієї інформації, здійснюється за ініціативою її власника. Але основною ознакою є те, що ця інформація, як зазначено в ч. 1. ст. 30 Закону України “Про інформацію”, перебуває у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб.

Детальніше правове регулювання питань комерційної таємниці визначено в новому Цивільному кодексі України (гл. 46 “Право власності на комерційну таємницю”²¹⁸).

Ст. 505 ЦК установлює такі ознаки комерційної таємниці:

- інформація є невідомою і не є легкодоступною для осіб, які зазвичай мають справу с інформацією такого роду;
- невідомість інформації іншим особам зумовлює її комерційну цінність;
- щодо інформації вжито заходів забезпечення її секретності;
- обмеження доступу до інформації здійснено особою яка володіє нею на законних підставах.

²¹⁸ Цивільний кодекс України від 16 січня 2003 р. // Відомості Верховної Ради України. – 2003. – № 40 – 44. – Ст. 356.

Нормами ст. 506 ЦК передбачено виключне право власника інформації, що становить комерційну таємницю на встановлення режиму доступу до цієї інформації; надання права на використання та перешкоджання неправомірному розголошенню, збиранню та використанню.

Аналогічна норма міститься і в ч. 2 ст. 30 Закону України “Про інформацію”, згідно з якою громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їхнього професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту.

Отже, суб’єктом визначення доступності інформації, становить комерційну таємницю, виступає власник відповідної інформації або особа якій надано право розпоряджатися цією інформацією на законних підставах, наприклад керівник підприємства.

Законодавство не містить чітко визначених строків обмеження доступу інформації, що становить комерційну таємницю, порядку надання відповідного грифу матеріальним носіям інформації, способів її захисту, порядку надання доступу до цієї інформації та обов’язків осіб, що отримали доступ до неї.

Усі ці аспекти визначає власник інформації на власний розсуд з урахуванням обмежень, установлених законодавством. З огляду на прямий зв’язок права на встановлення режиму доступу до комерційної таємниці із правом власності на інформацію, саме строком дії цього права (наприклад авторських прав) і обмежується строк дії відповідного режиму.

Одним із обмежень у віднесенні інформації до комерційної таємниці є визначення Кабінетом Міністрів України переліку відомостей, які не можуть становити комерційної таємниці. Згідно з даним переліком комерційну таємницю не становлять:

- установчі документи, документи, що дозволяють займатися підприємницькою чи господарською діяльністю та її окремими видами;
- інформація за всіма встановленими формами державної звітності;

- дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів;
- відомості про чисельність і склад працюючих, їхню заробітну плату в цілому та за професіями й посадами, а також наявність вільних робочих місць;
- документи про сплату податків і обов'язкових платежів;
- інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров'ю, а також інші порушення законодавства України та розміри заподіяних при цьому збитків;
- документи про платоспроможність;
- відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, спілках, об'єднаннях та інших організаціях, які займаються підприємницькою діяльністю;
- відомості, що відповідно до чинного законодавства підлягають оголошенню²¹⁹.

Установлення переліку відомостей, доступ до яких не може бути обмежений суб'єктами підприємницької діяльності, є однією з гарантій забезпечення поінформованості державних органів та громадськості про важливі аспекти їхньої діяльності.

Надаючи органам державної влади, відповідно до їх компетенції, інформацію, що становить таємницю, на них також покладають обов'язок дотримувати встановленого режиму обмеження доступу. Так, ст. 507 ЦК зобов'язує органи державної влади охороняти комерційну таємницю, яка надана ним у процесі їх діяльності.

Ще один механізм захисту інформації, що становить комерційну таємницю, визначено нормами ч. 4 ст. 25 Господарського кодексу України (ГК)²²⁰. які передбачають, обов'язок держави забезпечувати захист комерційної таємниці суб'єктів господарювання.

Неправомірне збирання, розголошення та використання комерційної таємниці розглядається як вид недобросовісної конкуренції, що вважається правопорушенням (ст. 32 ГК).

Українське законодавство передбачає кримінальну відповідальність за протиправні дії щодо інформації, що становить комерційну

²¹⁹ Про перелік відомостей, що не становлять комерційної таємниці: Постанова Кабінету Міністрів України від 9 серпня 1993 р. № 611.

²²⁰ Господарський кодекс України від 16 січня 2003 р. // Відомості Верховної Ради України. – 2003. – № 18. – Ст. 144.

таємницю. Так, ст. 231 Кримінального Кодексу України²²¹ передбачає відповідальність за незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю. Незаконними вважаються “умисні дії, спрямовані на отримання відомостей, що становлять комерційну таємницю, з метою розголошення чи іншого використання цих відомостей (комерційне шпигунство), а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб’єкту господарської діяльності”.

Інша Стаття 232 КК встановлює відповідальність за “умисне розголошення комерційної таємниці без згоди її власника особою, якій ця таємниця відома у зв’язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб’єкту господарської діяльності”.

Оскільки законодавство встановлює кримінальну відповідальність за розголошення та незаконний доступ до комерційної таємниці, для застосування цих механізмів правового захисту власник цієї інформації повинен встановлювати відповідні процедури визначення інформації комерційною таємницею та взяття з осіб, що отримують допуск до такої інформації, зобов’язань щодо її нерозголошення.

8. 3. Професійна таємниця

Закон України “Про інформацію” (ст. 30) називає “інформацією професійного характеру” і передбачає право фізичних та юридичних осіб захищати її. Існує істотна відмінність між комерційною та службовою таємницею. Щодо комерційної таємниці як правило, одна й та сама особа є і суб’єктом визначення доступності, і суб’єктом, що визначає заходи захисту такої інформації, причому і те й інше здійснює на власний розсуд. Розголошення або надання доступу до професійної таємниці перебуває у компетенції її власника, а обов’язки та відповідальність щодо її захисту несе особа, якій цю інформацію довірив власник у зв’язку з виконанням нею своїх професійних обов’язків, як правило, в інтересах власника інформації. Більше того, обов’язки особи щодо захисту професійної таємниці та запобігання її розголошенню без дозволу власника визначаються законодавством, яким регулюється відповідний вид професійної діяльності.

²²¹ Кримінальний кодекс України від 5 квітня 2001 р. // Там само. – 2001. – № 25-26 – Ст. 131.

Попри на те, що окремі види інформації, яка становить професійну таємницю, врегульовані правовими нормами різних галузей законодавства, існують певні загальні критерії віднесення інформації до професійної таємниці:

- інформація довірена або стала відомою особі виключно у зв'язку з виконанням нею своїх професійних обов'язків;
- особа, якій довірено інформацію, не перебуває на державній або муніципальній службі (в іншому випадку інформація вважається службовою таємницею);
- заборону на розповсюдження довіреної або такої, що стала відомою, інформації, яка може зашкодити правам або законним інтересам довірителя, встановлено законом;
- інформація не належить до відомостей, що становлять державну або комерційну таємницю.²²²

За такими критеріями розрізняють лікарську, адвокатську, нотаріальну, страхову, банківську та деякі інші види таємниці.

Особливі права і обов'язки у суб'єктів певних видів професійної діяльності виникають не просто так. Усі види професійної діяльності: (лікарської, адвокатської, нотаріальної, страхової, банківської та ін) виконують важливу суспільну функцію в громадянському суспільстві. Через це більшість перелічених видів професійної діяльності безпосередньо згадується в нормах Конституції України.

Саме великим суспільним значенням функцій названих видів професійної діяльності і зумовлене застосування додаткових заходів забезпечення цієї діяльності та прав й інтересів тих, хто звертається за їх послугами.

Особливістю правового регулювання професійної таємниці слід, також вважати те, що відповідні правила поведінки своїм виникненням зобов'язані не загальнолюдським моральним нормам, а нормам корпоративної моралі, або, як її ще називають, професійної етики. Ці норми виникли в процесі здійснення того чи іншого виду діяльності, і для людей, які не належать до відповідної професії, можуть бути неприйнятними. Найбільш яскравим і давнім прикладом професійної таємниці можна вважати **лікарську таємницю**, корені якої йдуть ще у Давній Греції і яка була викладена у клятві Гіппократа на межі V–IV ст.. до н.е.

²²² Бачило І. Л., Лопатин В. Н., Федотов М. А. Информационное право / Под. ред. акад. РАН Б. Н. Топорнина. – СПб.: Юрид. центр Пресс, 2001. – С. 538.

В Україні на законодавчому рівні лікарську таємницю закріплено в “Основах законодавства України про охорону здоров’я”. Ст. 40 цього Закону визначає, що “медичні працівники та інші особи, яким у зв’язку з виконанням професійних або службових обов’язків стало відомо про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя громадянина, не мають права розголошувати ці відомості, крім передбачених законодавчими актами випадків. При використанні інформації, що становить лікарську таємницю, в навчальному процесі, науково-дослідній роботі, в тому числі у випадках її публікації у спеціальній літературі, повинна бути забезпечена анонімність пацієнта”²²³.

Таким чином, особливістю лікарської таємниці є конфіденційність інформації щодо ідентифікації відомостей медичного характеру з конкретною людиною, за допомогою яких можна дізнатися про стан здоров’я конкретної особи.

З нормами, що регулюють лікарську таємницю, пов’язаний обов’язок лікаря надавати медичну інформацію (ст. 39 “Основ законодавства України про охорону здоров’я”). Згідно з нормами цієї статті, лікар зобов’язаний пояснити пацієнтові в доступній формі стан його здоров’я, мету запропонованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання, в т. ч. наявності ризику для життя і здоров’я. Пацієнт має право знайомитися з історією своєї хвороби та іншими документами, що можуть слугувати для подальшого лікування.

В особливих випадках, коли повна інформація може завдати шкоди здоров’ю пацієнта, лікар може її обмежити. В цьому разі він інформує членів сім’ї або законного представника пацієнта, враховуючи особисті інтереси хворого. Так само лікар діє, коли пацієнт перебуває в непритомному стані (ч. 3 ст. Основ)

Ця норма практично є єдиним випадком, коли людина може бути обмежена в отриманні персональної інформації про себе, яка не становить державної таємниці.

Аналогічні вимоги містить і Закон України “Про психіатричну допомогу”²²⁴. Зокрема, ст. 6 його передбачає, що медичні працівники, інші фахівці, які беруть участь у наданні психіатричної допомо-

²²³ Основи законодавства України про охорону здоров’я: Закон України від 19 листопада 1992 р. № 2801-XII // Відомості Верховної Ради. – 1993. – № 4. – Ст. 19.

²²⁴ Про психіатричну допомогу: Закон України від 22 лютого 2000 р. № 1489-III // Відомості Верховної Ради. – 2000. – № 19. – Ст. 143.

ги, та особи, яким у зв'язку з навчанням або виконанням професійних, службових, громадських чи інших обов'язків стало відомо про наявність в особи психічного розладу, про факти звернення за психіатричною допомогою та лікування у психіатричному закладі чи перебування в психоневрологічних закладах для соціального захисту або спеціального навчання, а також інші відомості про стан психічного здоров'я особи, її приватне життя, не можуть розголошувати ці відомості. Ця інформація може передаватися за згодою особи або її законного представника для проведення обстеження та лікування чи захисту її прав і законних інтересів, для здійснення наукових досліджень, публікацій в науковій літературі, використання у навчальному процесі. А також без зазначеної згоди для організації надання особі, яка страждає на тяжкий психічний розлад, психіатричної допомоги; для провадження дізнання, попереднього слідства або судового розгляду за письмовим запитом особи, яка проводить дізнання, слідчого, прокурора та суду.

Встановлена законодавством *адвокатська таємниця*, яку адвокат зобов'язаний зберігати, є однією із гарантій сумлінного виконання адвокатом своїх професійних обов'язків та забезпечення прав і законних інтересів його клієнта. Згідно ст. 9 Закону України "Про адвокатуру"²²⁵, предметом адвокатської таємниці є питання, з яких громадянин або юридична особа зверталися до адвоката, суть консультацій, порад, роз'яснень та інших відомостей, одержаних адвокатом при здійсненні своїх професійних обов'язків. Крім того, дані попереднього слідства, які стали відомі адвокату у зв'язку з виконанням ним своїх професійних обов'язків, можуть бути розголошені тільки з дозволу слідчого або прокурора. Адвокату, помічнику адвоката, посадовим особам адвокатських об'єднань забороняється розголошувати відомості, що становлять предмет адвокатської таємниці, і використовувати їх у своїх інтересах або в інтересах третіх осіб.

Слід зазначити, що *вимоги щодо збереження адвокатської таємниці не мають строку давності*, адже нормами ст. 10 Закону України "Про адвокатуру" взагалі забороняється вимагання від адвоката, його помічника, посадових осіб і технічних працівників адвокатських об'єднань відомостей, що становлять адвокатську таємницю.

²²⁵ Про адвокатуру: Закон України від 19 грудня 1992 р. № 2887-XII // Відомості Верховної Ради України. – 1993. – № 9. – Ст. 62.

Дотримання цієї норми забезпечується додатковими правилами, а саме:

- з питань, що становлять адвокатську таємницю, адвокати й технічні працівники адвокатських об'єднань не можуть бути допитані як свідки;
- документи, пов'язані з виконанням адвокатом доручення, не підлягають оглядові, розголошенню чи вилученню без його згоди.
- законом установлюється особливий порядок надання дозволу на прослуховування телефонних розмов адвокатів у зв'язку з оперативно-розшуковою діяльністю.

Адвокати, винні в розголошенні конфіденційних відомостей, що становлять адвокатську таємницю, несуть дисциплінарну відповідальність, а у разі розголошення ними без дозволу слідчого або прокурора даних попереднього слідства – і кримінальну відповідальність.

Найбільш детально правову й етичну природу професійної адвокатської таємниці викладено в Загальному кодексі правил для адвокатів країн Європейського Співтовариства²²⁶. Згідно з п. 2. 3. цього кодексу, особливість професії адвоката полягає в тому, що він одержує від клієнта відомості, які той не буде повідомляти іншій особі, а також іншу інформацію, яку йому належить зберігати в таємниці. Довіра до адвоката може виникнути лише за умови обов'язкового додержання ним принципу конфіденційності. Таким чином, конфіденційність є першорядним і фундаментальним правом та обов'язком адвоката.

Відповідно до цього режим конфіденційності інформації, пов'язаної з професійною діяльністю адвоката, визначається низкою правил:

- адвокат зобов'язаний однаковою мірою зберігати в таємниці як відомості, одержані ним від клієнта, так і інформацію про клієнта, надану йому у процесі надання послуг клієнту;
- на обов'язок додержання конфіденційності не поширюється дія строку давності;
- адвокат зобов'язаний вимагати додержання конфіденційності від помічників і від будь-яких інших осіб, які беруть участь у наданні послуг клієнту.

²²⁶ Загальний кодекс правил для адвокатів країн Європейського Співтовариства. Прийнято делегацією дванадцяти країн-учасниць на пленарному засіданні у Страсбурзі в жовтні 1988 р.

Тасмниця вчинюваних нотаріальних дій, як її визначена в норма ст. 8 Закону України “Про нотаріат”²²⁷, полягає в тому, що *нотаріуси та інші посадові особи, що вчиняють нотаріальні дії, зобов’язані додержувати тасмниці цих дій*. Зобов’язок додержання тасмниці вчинюваних нотаріальних дій поширюється також на осіб, яким про вчинені нотаріальні дії стало відомо у зв’язку з виконанням ними службових обов’язків.

Законом також передбачено деякі гарантії додержання нотаріальної тасмниці. Нормами тієї ж ст. 8 Закону України “Про нотаріат” визначено вичерпний перелік випадків розголошення цих відомостей. Так, довідки про вчинені нотаріальні дії та документи і копії з них видаються:

- тільки громадянам та юридичним особам, за дорученням яких або щодо яких вчинялися нотаріальні дії;
- на письмову вимогу суду, арбітражного суду, прокуратури, органів дізнання і слідства у зв’язку з кримінальними, цивільними або господарськими справами, що перебувають у їх провадженні;
- на письмову вимогу державної податкової адміністрації, необхідну для визначення правильності стягнення державного мита та цілей оподаткування;
- довідки про заповіти видаються тільки після смерті заповідача.

Законом передбачено відповідальність за порушення нотаріальної тасмниці.

Дуже схожою за своїми ознаками з нотаріальною є *тасмниця страхування*, передбачена Законом України “Про страхування”, у ст. 19 якого одним з обов’язків страхувальника (п. 6) названо “тримати в тасмниці відомості про страхувальника і його майновий стан, за винятком випадків, передбачених законодавством України”.²²⁸

8. 4. Банківська тасмниця

Ще одним специфічним видом конфіденційної інформації є *банківська тасмниця*. В Законі України “Про інформацію” (ст. 30) цей вид конфіденційної інформації названо поряд із професійною та ко-

²²⁷ Про нотаріат: Закон України від 2 вересня 1993 року № 3425-XII // Відомості Верховної Ради. – 1993. – № 39. – Ст. 383.

²²⁸ Про страхування: Закон України від 7 березня 1996 року № 85/96-ВР // Відомості Верховної Ради. – 1996. – № 18. – Ст. 78.

мерційною таємницями, що в принципі дає можливість розглядати банківську таємницю як самостійний вид конфіденційної інформації, хоча банківська таємниця має ті ж самі ознаки і природу, що й професійна. Так, ст. 60 Закону України “Про банки і банківську діяльність” визначає, що “інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту, є банківською таємницею”²²⁹.

Банківською таємницею, зокрема, є:

- відомості про стан рахунків клієнтів, у тому числі стан кореспондентських рахунків банків у Національному банку України;
- операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди; фінансово-економічний стан клієнтів;
- системи охорони банку та клієнтів;
- інформація про організаційно-правову структуру юридичної особи – клієнта, її керівників, напрями діяльності; відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;
- інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню; коди, що використовуються банками для захисту інформації.

Таким чином, банківська таємниця є специфічним видом конфіденційної інформації, що пов’язана з виконанням юридичними особами банківської діяльності та належністю фізичних осіб до відповідної професії – банківських службовців. Це цілком вкладається в рамки професійної таємниці, адже її суб’єктами є не тільки люди відповідної професії – лікарі, адвокати, працівники страхових компаній, але і юридичні особи – медичні заклади і установи, адвокатські фірми, об’єднання, страхові компанії тощо.

Законодавство визначає особливі вимоги для банківських установ щодо забезпечення відповідного правового режиму та вжиття заходів захисту інформації, що становить банківську таємницю.

Так, згідно зі ст. 61 Закону України “Про банки і банківську діяльність”, банки, зокрема, мають обов’язок щодо:

²²⁹ Про банки і банківську діяльність: Закон України від 7 грудня 2000 року № 2121-III // Відомості Верховної Ради. – 2001. – № 5-6. – Ст. 30.

- обмеження кола осіб, які мають доступ до інформації, що становить банківську таємницю;
- організації спеціального діловодства з документами, що містять банківську таємницю;
- застосування технічних засобів для запобігання несанкціонованому доступу до електронних та інших носіїв інформації;
- застосування застережень щодо збереження банківської таємниці та відповідальності за її розголошення у договорах і угодах між банком і клієнтом.

Законодавством встановлено також обов'язки і відповідальність осіб, які мають доступ до банківської таємниці, щодо дотримання режиму обмеження доступу:

- працівники банку в разі прийняття їх на роботу підписують зобов'язання щодо збереження банківської таємниці
- керівники та службовці банків зобов'язані не розголошувати та не використовувати з вигодою для себе чи для третіх осіб конфіденційну інформацію, яка стала відома їм при виконанні своїх службових обов'язків.
- аналогічний обов'язок щодо охорони довіреної їх банківської таємниці встановлено і щодо приватних осіб та організацій, які при виконанні своїх функцій або наданні послуг банку отримали інформацію, що є банківською таємницею.

У разі заподіяння розголошенням банківської таємниці шкоди інтересам банку чи клієнта вона підлягає відшкодуванню за рахунок особи, винної у її розголошенні.

Безпосередньо порядок організації обігу інформації, що становить банківську таємницю, визначено згідно з Постановою Національного банку України "Про затвердження Правил зберігання, захисту, використання та розкриття банківської таємниці"²³⁰.

Зокрема, цими правилами (п. 2. 1.) передбачено, що з метою забезпечення зберігання та захисту банківської таємниці банки зобов'язані у внутрішніх положеннях установити спеціальний порядок ведення діловодства з документами, що містять банківську таємницю, зокрема визначити: порядок реєстрації вихідних документів, роботи з документами, що містять банківську таємницю, відправлення та зберігання документів, які містять банківську таємницю, а

²³⁰ Про затвердження Правил зберігання, захисту, використання та розкриття банківської таємниці: Постанова Національного банку України від 14 липня 2006 р. № 267.

також особливості роботи з електронними документами, які містять банківську таємницю.

Потреба проставлення на документах грифу “Банківська таємниця” визначається відповідним виконавцем під час опрацювання вхідних документів банку. Наявність на документах та інших матеріальних носіях інформації грифу “Банківська таємниця” зумовлює застосування подальших заходів захисту інформації. Так, під час роботи з документами, що містять гриф “Банківська таємниця”, працівники банку мають забезпечити зберігання таких документів у сейфах або шафах, які надійно замикаються і до яких не мають доступу треті особи.

Банки зобов’язані під час відправлення (передавання) інформації, що містить банківську таємницю, забезпечити її гарантовану доставку та конфіденційність. Забороняється відправлення документів із грифом “Банківська таємниця” з використанням факсимільного зв’язку або іншими каналами зв’язку, що не забезпечують захисту інформації.

Автоматизовані системи, які обробляють інформацію, що містить банківську таємницю, мають створюватися банками так, щоб обмежити доступ користувачів лише в межах, необхідних для виконання їх службових обов’язків.

Одним із елементів забезпечення захисту інформації, що становить банківську таємницю, є визначені законодавством особливі підстави та процедура розкриття банками такої інформації. Так, згідно зі ст. 62 Закону України “Про банки та банківську діяльність”, інформація про юридичних та фізичних осіб, яка містить банківську таємницю, розкривається банками:

1) на письмовий запит або з письмового дозволу власника такої інформації;

2) на письмову вимогу суду або за рішенням суду;

3) органам прокуратури України, Служби безпеки України, Міністерства внутрішніх справ України, Антимонопольного комітету України, Державної податкової служби України (з питань оподаткування або валютного контролю);

5) спеціально уповноваженому органу виконавчої влади з питань фінансового моніторингу на його письмову вимогу або у разі виникнення підозр;

6) органам державної виконавчої служби на їх письмову вимогу з питань виконання рішень судів.

Відповідно до зазначених “Правил зберігання, захисту, використання та розкриття банківської таємниці”, затверджених НБУ, отримавши запит про розкриття інформації, що становить банківську таємницю, банк зобов’язаний розкрити цю інформацію або дати мотивовану відповідь про неможливість надання відповідної інформації протягом 10 робочих днів з дня отримання вимоги.

Важливою вимогою при розкритті інформації, що становить банківську таємницю, є те, що банку дозволяється надавати відомості лише щодо конкретної юридичної або фізичної особи, зазначеної у запиті, та лише у випадку, якщо ця особа є клієнтом цього банку. Розкриття ж інформації про інших осіб не допускається.

Так, банку забороняється надавати інформацію про клієнтів іншого банку, навіть якщо вони зазначені в документах, договорах та операціях клієнта, якщо інше не зазначено в дозволі клієнта іншого банку або вимозі, рішенні (постанові) суду.

Крім того, під час надання інформації про операції за рахунками конкретної юридичної особи або фізичної особи – суб’єкта підприємницької діяльності за конкретний проміжок часу банк надає інформацію про рух коштів на рахунок клієнта без зазначення контрагентів за операціями.

ГЛАВА 9 ПРАВОВІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ

Основні принципи діяльності із захисту інформації. Захист інформації в інформаційних системах. Технічний захист інформації. Криптографічний захист інформації. Національна система конфіденційного зв'язку. Державна служба спеціального зв'язку та захисту інформації України.

9. 1. Основні принципи діяльності із захисту інформації

Питання захисту інформації є важливим у забезпеченні дотримання відповідних режимів інформаційних ресурсів та доступу до інформації. Слід зазначити, що захист може здійснюватися щодо інформації з будь-яким видом режиму доступу, але мета і завдання такого захисту будуть різними відповідно до вимог відповідного режиму. Зокрема, про таку особливість йдеться у Правилах забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Кабінетом Міністрів України²³¹, якими розрізняються вимоги до захисту відкритої інформації та інформації з обмеженим доступом.

Основною вимогою до захисту відкритої інформації є *збереження її цілісності*, що забезпечується захистом від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення. Відповідно дотримання режиму доступу до такої інформації передбачає, що:

- усім користувачам має бути забезпечений доступ до ознайомлення з відкритою інформацією;
- модифікація або знищення відкритої інформації може здійснюватися лише користувачами, яким надано відповідні повноваження;
- спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, повинні блокуватися.

²³¹ Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373.

Захист конфіденційної і таємної інформації передбачає здійснення комплексу організаційних та правових заходів, які забезпечують вирішення низки завдань, до яких належить захист відповідної інформації від: 1) несанкціонованого та неконтрольованого ознайомлення; 2) модифікації; 3) знищення; 4) копіювання; 5) поширення.

Відповідно забезпечення дотримання режиму доступу до таємної або конфіденційної інформації передбачає, що:

- доступ до конфіденційної інформації надається тільки користувачам, які мають на це повноваження;
- спроби доступу до такої інформації осіб чи користувачів, які не мають відповідних повноважень повинні блокуватися;
- користувачеві може надаватися право на виконання однієї або кількох конкретних операцій з обробки конфіденційної інформації або він може бути позбавлений такого права.

Захист інформації зазвичай здійснюється в рамках певних інформаційних систем. Із правового погляду вони становлять “організаційно впорядковану сукупність документів (масивів документів) і інформаційних технологій, в тому числі з використанням засобів обчислювальної техніки і зв’язку, які реалізують інформаційні процеси”²³². Цілком логічним сприймається застереження “в тому числі” стосовно комп’ютерних технологій. Адже автоматизовані засоби оброблення інформації з’явилися за історичними мірками зовсім недавно. І навпаки, протягом кількох тисячоліть існують традиційні способи оброблення та передачі інформації. Вже з початку XX ст. до них поступово додалися телеграфні, телефонні, радіо, телевізійні, комп’ютерні мережі передачі інформації. Слід зазначити, що відповідні цілі діяльності із захисту інформації є універсальними і не залежать від виду інформаційної системи, інформаційного ресурсу або фізичного носія інформації. Адже загальні вимоги однакові до як інформаційних ресурсів так і електронних, паперових та інших фізичних носіїх.

Захист інформації є комплексною категорією, що зумовлена багатьма чинниками. Будь-яка інформаційна система, особливо автоматизована, “поділяється на функціональну частину та частину забезпечення, кожна з яких поділяється на складові елементи мінімально можливої розмірності”.²³³ Функціональна частина інформаційної системи виконує функції і завдання, що підлягають реалізації за до-

²³² Копылов В. А. Информационное право. – 2-е изд., перераб. и доп. – М.: Юристъ, 2002. – с. 63.

²³³ Копылов В. А. Информационное право. – М.: Юристъ, 1997. – с. 152.

помогою цієї системи. Частина забезпечення представляє – це “наповнення” функціональної частини, за допомогою якого фактично реалізуються функції і завдання системи. Узагальнюючи такий підхід, можна говорити, що інформаційна система функціонує за тими самими правилами й законами, що і будь-який інший вид систематизованої діяльності з розподілом ролей і функцій. Створення будь-якої системи оброблення чи передавання інформації, починаючи від поштової служби і закінчуючи комп’ютерними мережами, охоплює величезну кількість етапів та елементів. До переліку їх належать: створення фізичних об’єктів на яких ця система розміщується; створення технічного і програмного забезпечення; підготовка кадрів; забезпечення фінансовими та енергетичними ресурсами тощо. І загрози, які усуває або яким запобігає система заходів захисту інформації, можуть виникати на будь-якому етапі створення чи експлуатації інформаційної системи.

Винятково важливою є проблема визначення конкретних чинників, які потрібно враховувати, щоб охарактеризувати безпечність конкретну інформаційну систему. Для цього потрібно зважати на функціональне призначення систем та об’єктів інформаційної системи. Головне їх завдання полягає у реалізації інформаційних процесів. Тому цінною є насамперед та інформація, що обробляється в цих системах. Отже, інформаційна інфраструктура має забезпечувати інформацію або інформаційні ресурси, які обробляються, від “потенційно, або реально можливих дій, що призводять до неправомірного заволодіння відомостями що охороняються”.²³⁴

Неправомірними зокрема, можуть бути такі дії:

- ознайомлення з конфіденційною інформацією різними шляхами і способами без порушення її цілісності;
- модифікація інформації в протиправних цілях як часткова або значна зміна складу і змісту відомостей;
- руйнування (знищення) інформації як акт вандалізму або з метою заподіяння прямої матеріальної шкоди.

Результатом неправомірних дій з інформацією є “порушення її конфіденційності, повноти, достовірності та доступності, що, у свою чергу, призводить до порушення як режиму управління, так і його якості в умовах спотвореної або неповної інформації”²³⁵.

²³⁴ Ярочкин В. И. Информационная безопасность. – М. : Междунар. отношения, 2000. – С. 17.

²³⁵ Там само. – С. 18.

Таким чином, можна стверджувати, що головним об'єктом загрози для інформаційної системи є суспільні відносини які складаються з приводу управління і користування об'єктами. А безпосередній предмет загрози – інформаційні ресурси та інформація, що обробляється. Отже, щодо безпеки інформаційна інфраструктура є певною оболонкою, яка захищає інформацію, що міститься в ній, від негативного впливу зовнішніх чинників.

Останні можна поділити за джерелами на три групи²³⁶:

Антропогенні (безпосередньо створені людьми):

- ненавмисні або навмисні діяння обслуговуючого і управлінського персоналу, програмістів, користувачів, служби безпеки інформаційної системи;
- дії несанкціонованих користувачів (діяльність іноземних розвідувальних і спеціальних служб, кримінальних структур, недобросовісних партнерів та конкурентів, а також протиправна діяльність інших окремих осіб).
- Техногенні (зумовлені випадковим впливом технічних об'єктів):
- внутрішні (неякісні технічні і програмні засоби оброблення інформації; засоби зв'язку, охорони, сигналізації; інші технічні засоби, що застосовуються в установі);
- глобальні техногенні загрози (небезпечні виробництва, мережі енерго-, водопостачання, каналізації, транспорт тощо), які призводять до зникнення або коливання електропостачання та інших засобів забезпечення і функціонування, відмов та збоїв апаратно-програмних засобів;
- електромагнітні випромінювання і наведення, витоки через канали зв'язку (оптичні, електричні, звукові) тощо.

Природні (вплив негативних природних чинників) – стихійні лиха, магнітні бурі, радіоактивний вплив.

Звідси для інформаційної структури взагалі і для кожного її об'єкта, зокрема важливим є забезпечити незмінність внутрішніх умов оброблення інформації за одночасної зміни (в т. ч. і негативного) зовнішніх умов.

Отже, *безпеку інформаційних систем можна охарактеризувати як стан забезпеченості необхідних умов і параметрів інформаційних*

²³⁶ Див. напр.: Бачило І. Л., Лопатин В. Н., Федотов М. А. Информационное право / Под ред. акад. РАН Б. Н. Топорнина. – СПб.: Юрид. центр Пресс, 2001. – С. 643.

процесів, що реалізуються за їх допомогою, від негативного впливу ззовні.

Відомі два способи регулювання питань захисту інформації. Перший забезпечується державною власністю на найважливіші (стратегічні) інформаційні системи та інформаційні ресурси і полягає в безпосередньому державному управлінні відповідними об'єктами. Другий забезпечується юрисдикцією держави на власній території і полягає в запровадженні єдиних, обов'язкових стандартів інформаційних процесів, яких мають дотримуватися власники або оператори об'єктів інформаційної інфраструктури.

Загалом, коли йдеться про захист інформації, більшість дослідників погоджується з тим, що цей захист може бути лише комплексним. Але в цій комплексній системі можна виділити спектр напрямів діяльності суб'єктів захисту інформації, які характеризуються специфічними методами і способами захисту інформації. Зазвичай виокремлюють:

- правовий захист – спеціальні закони, інші нормативні акти, правила, процедури і заходи, що забезпечують захист інформації на правовій основі;
- організаційний захист – регламентація виробничої діяльності і взаємовідносин виконавців на нормативно-правовій основі, що виключає або послаблює завдання будь-якої шкоди виконавцям;
- інженерно-технічний захист – використання різних технічних засобів, що запобігають спричиненню шкоди інформації.²³⁷

Зазначимо, що в будь-якому разі основу всіх перелічених вище заходів становлять правові норми, якими регламентується діяльність у сфері захисту інформації. Крім того, правовий захист інформації, який було розглянуто в попередніх розділах, стосується, так би мовити, інформації в “чистому” вигляді, незалежно від її носія. А от наступні – організаційний і інженерно-технічний аспекти захисту інформації спрямовані не безпосередньо на інформацію, а на системи, об'єкти та носії, на яких ця інформація збирається, обробляється й розповсюджується.

²³⁷ Див.: Ярочкин В. И. Информационная безопасность. – М. : Международные отношения, 2000. – с. 32 – 33.

9. 2. Захист інформації в інформаційних системах

Нині найбільш актуальним безумовно, є захист інформації, поданої в електронній формі, адже саме цей вид її, з огляду на нематеріальний характер, високу здатність до трансформації й передачі є найбільш вразливим до протиправних дій. Інформація в електронній формі обробляється, передається та розповсюджується за допомогою інформаційно-телекомунікаційних систем, будучи їх основним наповненням. В Україні останнім часом створено достатньо широку нормативно-правову базу для проведення діяльності із захисту цього виду інформації. Причому можна виділити два аспекти захисту інформації в інформаційно-телекомунікаційних системах: 1) встановлення стандартів і вимог щодо характеристик інформаційних систем, які мають забезпечувати дієвість цієї системи; безпосереднє правове регулювання діяльності із захисту інформації.

Наприклад, Закон України “Про телекомунікації” (ст. 1) виділяє дві характеристики безпеки інформаційних систем і мереж.

1) *інформаційна безпека телекомунікаційних мереж* – здатність мереж забезпечувати захист від знищення, перекручування, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації.

2) *сталість телекомунікаційної мережі* – властивості телекомунікаційної мережі зберігати повністю або частково свої функції у разі впливу на неї дестабілізаційних чинників.

Ст. 9 Закону України “Про телекомунікації” визначено обов’язки операторів і провайдерів телекомунікацій щодо забезпечення відповідних характеристик і властивостей засобів телекомунікацій.

Правовою основою діяльності із захисту інформації є Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”²³⁸. Відповідно до ст. 1 цього Закону, *захист інформації в системі – це діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі*.

Сама ж автоматизована система є такою, що виконує автоматизоване оброблення даних і в складі якої є технічні засоби їх оброблення (засоби обчислювальної техніки і зв’язку), а також методи і процедури, програмне забезпечення.

²³⁸ Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 31 травня 2005 р. № 2594-IV // Відомості Верховної Ради України. – 2005. – № 26. – Ст. 347.

Закон виначає п'ять основних видів несанкціонованих дій з інформацією:

- 1) блокування інформації в системі – дії, внаслідок яких унеможливується доступ до інформації в системі;
- 2) виток інформації – результат дій, внаслідок яких інформація в системі стає відомою або доступною фізичним та/або юридичним особам, що не мають права доступу до неї;
- 3) знищення інформації в системі – дії, внаслідок яких інформація в системі зникає;
- 4) порушення цілісності інформації в системі – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її зміст.

Важливим аспектом інформаційної безпеки є захист інформації яка передається, зберігається та обробляється за допомогою комунікаційних систем різних типів. Щодо цього в Україні вже створено низку нормативно-правових актів.

Об'єктами захисту від неправомірних зазіхань є:

- інформація, що обробляється в автоматизованій системі;
- права власників цієї інформації та власників автоматизованої системи;
- права користувача.

Захист інформації полягає у застосуванні сукупності організаційно-технічних заходів і правових норм для запобігання заподіяння шкоди інтересам власника інформації чи автоматизованої системи та особам, які користуються інформацією.

Закон України “Про захист інформації в автоматизованих системах” визначає: також відносини між суб'єктами в процесі оброблення інформації в автоматизованих системах, загальні вимоги до захисту інформації в АС і порядок організації цього захисту, відповідальність за порушення норм цього закону та засади міжнародної співпраці України у сфері автоматизованих систем.

Зазначимо, що конкретний зміст вимог до захисту інформації належить насамперед від права власності на конкретну інформації, що обробляється за допомогою автоматизованої системи. Так, за ст. 11 Закону України “Про захист інформації в автоматизованих системах”, вимоги і правила захисту інформації, яка є власністю держави, або інформації, захист якої гарантується державою, визначаються відповідними нормативно-правовими актами. Ці вимоги є обов'язковими для власників автоматизованих систем, де така інформація обробляється,

а для інших суб'єктів права власності на інформацію такі вимоги мають лише рекомендаційний характер.

Політика із захисту інформації в автоматизованих системах визначається Верховною Радою України, а державне управління в цій сфері здійснює Кабінет Міністрів України.

Державне управління у сфері захисту інформації в автоматизованих системах передбачає:

- проведення єдиної технічної політики захисту інформації;
- розроблення концепції, вимог, нормативно-технічних документів і науково-методичних рекомендацій захисту інформації в автоматизованих системах;
- затвердження порядку організації, функціонування та контролю за виконанням заходів захисту оброблюваної в автоматизованій системі інформації, яка є власністю держави, а також рекомендацій щодо захисту інформації – власності юридичних та фізичних осіб;
- організації випробувань і сертифікації засобів захисту інформації в автоматизованих системах, в якій здійснюється обробка інформації, що власністю держави;
- створення відповідних структур для захисту інформації в автоматизованих системах;
- проведення атестації сертифікаційних (випробувальних) органів, центрів і лабораторій, видача ліцензії на право проведення сервісних робіт в галузі захисту інформації в автоматизованих системах;
- здійснення контролю захищеності оброблюваної в автоматизованих системах інформації, яка є власністю держави;
- визначення порядку доступу осіб і організацій зарубіжних держав до інформації в автоматизованих системах, яка є власністю держави, або до інформації – власності фізичних та юридичних осіб, щодо поширення і використання якої державою встановлено обмеження.

Нормами законодавства встановлено комплексний характер захисту інформації. Зокрема, захист державних інформаційних ресурсів в автоматизованих системах, що належать до інформаційно-телекомунікаційних систем, здійснюється через запровадження комплексної системи захисту інформації (КСЗІ). Ця система складається з комплексу технічних, криптографічних, організаційних та інших

заходів і засобів, спрямованих на запобігання блокуванню інформації, несанкціонованому ознайомленню з нею та/або її модифікації²³⁹.

Основними в комплексній системі захисту інформації є технічний та криптографічний захист, а також комплекс заходів організаційного характеру, який передбачає встановлення відповідних режимів діяльності об'єктів інформаційних систем, контроль за дотриманням правил і норм здійснення захисту інформації, контроль за діяльністю суб'єктів захисту інформації тощо.

9. 3. Технічний захист інформації

Згідно з Положенням “Про технічний захист інформації в Україні”, яке було затверджене Указом Президента, *технічний захист інформації (ТЗІ) – це діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації*²⁴⁰.

Комплекс заходів технічного захисту інформації може бути здійснений лише в інформаційній системі або на іншому об'єкті інформаційної інфраструктури. Рівень безпеки інформації, яка обробляється в системах та на об'єктах інформаційної інфраструктури визначається комплексом таких її властивостей:

- конфіденційність – властивість інформації бути захищеною від несанкціонованого ознайомлення;
- цілісність – властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;
- доступність – властивість інформації бути захищеною від несанкціонованого блокування.

Лише наявність цих трьох характеристик інформації, що підлягає захисту, є умовою ефективного і безпечного використання суб'єктами інформаційних процесів необхідних об'єктів інформаційної інфраструктури.

В Україні введено державне регулювання діяльності із ТЗІ, яке передбачає:

- ліцензування та надання дозволів на провадження діяльності із ТЗІ;

²³⁹ Див. : Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах: Наказ ДСТСЗІ СБУ від 24 грудня 2001 р. № 76.

²⁴⁰ Про Положення про технічний захист інформації в Україні: Указ Президента України від 27 вересня 1999 р. № 1229.

- сертифікацію та державне експертне оцінювання продукції у сфері ТЗІ.

Процедура надання ліцензії або дозволу визначається змістом завдань, які вирішуються в межах діяльності з ТЗІ:

1) організації, які виконують діяльність з ТЗІ з метою надання відповідних послуг іншим фізичним та юридичним особам, повинні отримати ліцензію на право проведення господарської діяльності у галузі ТЗІ;

2) органи державної влади та місцевого самоврядування, які здійснюють роботи з ТЗІ для власних потреб, отримують право на їх проведення у дозвільному порядку²⁴¹.

Нині ліцензування діяльності в галузі ТЗІ та контроль за додержанням ліцензійних вимог здійснюють адміністрацією Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку). Правила ліцензування цього виду господарської діяльності визначаються "Ліцензійними умовами провадження господарської діяльності, пов'язаної з розробленням, виробництвом, впровадженням, обслуговуванням, дослідженням ефективності систем і засобів технічного захисту інформації, наданням послуг у галузі технічного захисту інформації"²⁴².

Усього в галузі ТЗІ підлягає ліцензуванню 7 видів робіт, а саме:

- 1) розроблення, впровадження, дослідження ефективності, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є акустичні поля, надання консультативних послуг;
- 2) розроблення, впровадження, дослідження ефективності, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є електромагнітні поля та електричні сигнали, надання консультативних послуг;
- 3) розроблення, виробництво, впровадження, дослідження ефективності, супроводження засобів та комплексів технічного захисту інформації в інформаційних системах, інформаційних технологій із захистом інформації від несанкціонованого доступу, надання консультативних послуг;

²⁴¹ Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб: Наказ ДСТСЗІ СБУ від 23 лютого 2002р. № 9.

²⁴² Про затвердження ліцензійних умов провадження господарської діяльності, пов'язаної з розробленням, виробництвом, впровадженням, обслуговуванням, дослідженням ефективності систем і засобів технічного захисту інформації, наданням послуг у галузі технічного захисту інформації: Спільний наказ Держкомпідприємництва та ДСТСЗІ СБУ від 29 грудня 2000 р. № 89/67.

- 4) виявлення та блокування витоку мовної та видової інформації через закладні пристрої на об'єктах інформаційної діяльності, надання консультативних послуг;
- 5) виробництво засобів забезпечення технічного захисту інформації, носіями якої є акустичні поля;
- 6) виробництво засобів забезпечення технічного захисту інформації, носіями якої є електромагнітні поля та електричні сигнали;
- 7) розроблення, впровадження, дослідження ефективності, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є хімічні речовини, надання консультативних послуг.

Для органів державної влади та органи місцевого самоврядування Держспецзв'язку надає дозволи на проведення робіт з технічного захисту інформації для власних потреб і здійснює контроль за проведенням ними визначених видів робіт.

Система оцінювання продукції у сфері ТЗІ, як уже зазначалося, складається з двох процедур – сертифікації засобів ТЗІ та державної експертизи.

Об'єктом *сертифікації в галузі ТЗІ* є окремі засоби ТЗІ. Сертифікації підлягають:

- засоби ТЗІ, які виробляються серійно;
- одиничні зразки засобів ТЗІ;
- засоби ТЗІ імпортного виробництва.

Процедура сертифікації полягає наданні споживачеві засобів ТЗІ гарантії відповідності цих засобів нормативним документам. Порядок та вимоги до проведення сертифікації засобів ТЗІ визначаються Наказом Держстандарту України “Про затвердження Порядку проведення робіт з сертифікації засобів забезпечення технічного захисту інформації загального призначення”²⁴³.

Сертифікація засобів ТЗІ в Україні здійснюється органами та випробувальними лабораторіями, які є акредитованими в Українській державній системі сертифікації продукції (УкрСЕПРО).

Державна експертиза у сфері ТЗІ здійснюється відповідно до Закону України “Про наукову і науково-технічну експертизу”²⁴⁴ та від-

²⁴³ Про затвердження Порядку проведення робіт з сертифікації засобів забезпечення технічного захисту інформації загального призначення: Наказ Держстандарту України від 9 липня 2001 р. № 329/32

²⁴⁴ Про наукову і науково-технічну експертизу: Закон України від 10 лютого 1995 р. № 51/95-ВР // Відомості Верховної Ради України. – 1995. – № 9. – Ст. 56.

повідного “Положення про державну експертизу в сфері технічного захисту інформації”²⁴⁵.

Замовником державної експертизи у сфері ТЗІ є Держспецзв’язком.

Організаторами експертизи є фізичні та юридичні особи, які на підставі доручення або договору із замовниками організовують та проводять експертизу і подають експертні висновки.

Експертами є фізичні особи, які мають високу кваліфікацію, спеціальні знання і безпосередньо здійснюють наукову чи науково-технічну експертизу та несуть персональну відповідальність за достовірність і повноту аналізу, обґрунтованість рекомендацій відповідно до вимог завдання на проведення експертизи.

Організатори експертизи та експерти, яким надано право здійснювати державну експертизу в сфері ТЗІ, підлягають реєстрації у відповідному Реєстрі.

Результати проведеної державної експертизи у сфері ТЗІ оформляються у вигляді *експертних висновків*, які видаються щодо окремих засобів технічного захисту інформації, та *атестатів відповідності*, які видаються на комплексні системи захисту інформації в інформаційно-телекомунікаційних системах.

Наявність позитивного експертного висновку щодо засобу ТЗІ є підставою для його включення до Переліку засобів технічного захисту інформації загального призначення, які дозволені до використання з метою ТЗІ.

Наявність атестату відповідності є обов’язковою умовою надання власникові інформаційно-телекомунікаційної системи дозволу на оброблення в цій системі інформації, що підлягає захисту, відповідно до вимог законодавства.

Отже, система державного регулювання у сфері технічного захисту інформації має комплексний характер і забезпечується встановленням відповідних правил і стандартів, які стосуються як діяльності у сфері ТЗІ, що включають ліцензування та надання відповідних дозволів, так і спеціальними вимогами до засобів ТЗІ та інформаційно-телекомунікаційних систем, які включають стандартизацію, сертифікацію та атестацію.

²⁴⁵ Про затвердження Положення про державну експертизу в сфері технічного захисту інформації: Наказ ДСТСЗІ СБУ від 29 грудня 1999 р. № 62.

9. 4. Криптографічний захист інформації

Криптографічний захист інформації є найдавнішим, оскільки його корені сягають ще IV тисячоліття до н. е. , коли в давньому Єгипті, Шумері, Китаї, Індії та Ассирії виникли перші шифри. Але основоположником криптографічної науки вважається К. Шенон, який у 1946 р. видав працю під назвою “Теорія зв’язку в секретних системах”, у якій виклав теоретичні основи сучасної криптографії. Саме відтоді застосування криптографічного захисту інформації стало швидко поширюватися не лише у військово-політичній сфері, а й у промисловості, банківській діяльності, приватній кореспонденції тощо.

Криптографія стала справою не лише спецслужб, як би вони того не бажали. У 70 – 80-ті роки. XX ст. підвищується суспільний інтерес до криптографії. Виявилося, що криптографічні засоби можуть бути добрим інструментом захисту прав громадян на конфіденційність листування і переговорів. Цьому сприяло відкриття односторонніх функцій і криптографії з відкритими ключами, так званих “хеш-функцій” (спеціальних ознак повідомлень, за якими легко ідентифікувати повідомлення і виявити його модифікації); механізмів цифрового підпису (аналога звичайного рукописного підпису, який надає електронним документам юридичної сили) тощо.²⁴⁶

В Україні нормативно-правове регулювання питань криптографічного захисту інформації розвивається досить швидко. Основою цього виду діяльності є затверджене Указом Президента “Положення про порядок здійснення криптографічного захисту інформації”, згідно з яким *криптографічний захист інформації є таким, що здійснюється за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо*²⁴⁷.

Цей Указ визначає основні терміни, що використовуються у криптографічному захисті інформації:

- *засіб криптографічного захисту інформації* – програмний, апаратно-програмний, апаратний або інший засіб, призначений для криптографічного захисту інформації;

²⁴⁶ Див.: Потій О. Криптография, прошлое и настоящее // Служба безопасности. – 2001. – № 2 - 3. – С. 28 – 30.

²⁴⁷ Про Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ Президента України від 22 травня 1998 р. № 505/98.

- *криптографічна система (криптосистема)* – сукупність засобів криптографічного захисту інформації, необхідної ключової, нормативної, експлуатаційної, а також іншої документації (у тому числі такої, що визначає заходи безпеки), використання яких забезпечує належний рівень захищеності інформації, що обробляється, зберігається та (або) передається.

Сам же криптографічний захист інформації здійснюється за допомогою відповідної криптосистеми, яка складається із сукупності органів, підрозділів, груп, діяльність яких спрямована на забезпечення криптографічного захисту інформації, та підприємств, установ і організацій, що розробляють, виробляють, експлуатують та (або) розповсюджують криптосистеми і засоби криптографічного захисту інформації.

Конкретні вимоги до засобів криптографічного захисту інформації залежать від правового режиму останньої та її суспільного і державного значення.

Так, для криптографічного захисту інформації, що становить державну таємницю, та службової інформації, створеної на замовлення державних органів або яка є власністю держави, використовуються криптосистеми і засоби криптографічного захисту, допущені до експлуатації Держспецзв'язку. Такі криптосистеми і засоби перебувають виключно у державній власності.

Проте засоби криптографічного захисту службової інформації та криптосистеми з відповідного дозволу можуть перебувати і в недержавній власності.

Щодо криптосистем і засобів криптографічного захисту конфіденційної інформації встановлено лише вимогу наявності сертифікату відповідності.

Законодавством також встановлено вимоги щодо ліцензування діяльності, пов'язаної з розробленням, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів криптографічного захисту інформації, а також з наданням послуг із криптографічного захисту інформації.

Надійність криптографічного захисту інформації забезпечують не лише якість та характеристики самих криптосистем, а й організаційні заходи, які унеможливають витік інформації, що може допомогти у зламі криптографічного захисту. З цією метою встановлено особливий порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації та постачання і використання ключів до цих засобів.

Заходи організаційного забезпечення криптографічного захисту інформації (КЗІ) проводяться через установлення:

- режиму безпеки тобто реалізованої системи правових норм, організаційних та організаційно-технічних заходів, яка створюється на підприємствах під час розроблення, дослідження, виробництва та експлуатації засобів КЗІ з метою обмеження доступу до конфіденційної інформації;
- спеціальних вимог до КЗІ, тобто вимог до принципів побудови засобів КЗІ і технічної реалізації криптографічних алгоритмів у засобах КЗІ, до криптографічних якостей, а також до захисту від можливих каналів витоку небезпечних сигналів засобів КЗІ.²⁴⁸

Головними вимогами до інформаційної безпеки засобів КЗІ є такі:

- особи, допущені до розроблення, виготовлення та експлуатації КЗІ, повинні мати допуск, відповідний рівневі таємної або конфіденційної інформації, яку передбачається захищати такими засобами КЗІ;
- у засобах КЗІ мають використовуватися криптоалгоритми та криптопротоколи, які є державними стандартами України або рекомендовані Держспецзв'язку;
- засоби КЗІ без уведених діючих ключових даних мають гриф обмеження доступу, який відповідає грифу опису криптосхеми;
- гриф обмеження доступу засобів КЗІ із завантаженими ключовими даними визначається грифом обмеження доступу ключових документів;
- гриф обмеження доступу ключових документів, що використовуються засобами КЗІ, має відповідати максимальному грифу обмеження доступу інформації, яка захищається.

Порядок постачання і використання ключів до засобів КЗІ, та відповідні організаційні й технічні заходи безпеки регулюються спеціальною інструкцією, затвердженою спільним наказом Держстандарту та СБУ, якою запроваджено “єдині вимоги, обов’язкові для виконання юридичними особами будь-яких форм власності, що передбачені чинним законодавством”²⁴⁹.

²⁴⁸ Про затвердження Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації: Наказ ДСТСЗІ СБУ 30 листопада 1999 р. № 53.

²⁴⁹ Про затвердження Тимчасової інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації: Наказ Держстандарту України та Служби безпеки України від 28 листопада 1997 р. № 708/156.

9. 5. Національна система конфіденційного зв'язку

Одним із напрямів забезпечення захисту інформації з обмеженим доступом стало створення в Україні загальнонаціональної спеціальної інформаційно-телекомунікаційної системи, яка дістала назву Національна система конфіденційного зв'язку.

Згідно з нормами ст. 1 Закону України “Про Національну систему конфіденційного зв'язку”²⁵⁰, *Національна система конфіденційного зв'язку – сукупність спеціальних телекомунікаційних систем (мереж) подвійного призначення, які за допомогою криптографічних та/або технічних засобів забезпечують обмін конфіденційною інформацією в інтересах органів державної влади та органів місцевого самоврядування, створюють належні умови для їх взаємодії в мирний час та у разі введення надзвичайного і воєнного стану.*

Основними складовими елементами НСКЗ є:

- спеціальні телекомунікаційні системи (мережі), призначені для обміну інформацією з обмеженим доступом;
- фіксовані й мобільні компоненти відповідних телекомунікаційних систем;
- централізовані системи захисту інформації та оперативно-технічного управління.

Державну підтримку НСКЗ, яка полягає у створенні шляхом створення сприятливих правових, економічних та інших умов, здійснює Кабінет Міністрів України.

Управління НСКЗ, її функціонування, розвиток, використання та захист інформації забезпечуються Адміністрацією Державної служби спеціального зв'язку та захисту інформації України (Адміністрація Держспецзв'язку).

Суб'єктами цієї системи, які беруть участь у її створенні, функціонуванні, розвитку та використанні, можуть бути як органи публічної влади, так і фізичні та юридичні особи, які можуть бути власниками окремих компонентів НСКЗ.

Але, згідно із законодавством, такі компоненти НСКЗ, як централізовані системи захисту інформації та оперативно-технічного управління, перебувають виключно в державній власності і не підлягають приватизації.

²⁵⁰ Про Національну систему конфіденційного зв'язку: Закон України від 10 січня 2002 р. № 2919-III // Відомості Верховної Ради України – 2002 – № 15. – Ст. 103.

Послуги конфіденційного зв'язку за допомогою НСКЗ надаються операторами, які є юридичними особами і мають ліцензії на право надання послуг фіксованого та/або рухомого (мобільного) телефонного зв'язку, а також надання послуг у галузі криптографічного та/або технічного захисту інформації відповідно до законодавства.

Абонентами цієї системи можуть бути як органи державної влади та місцевого самоврядування, так і юридичні та фізичні особи, які отримують відповідні послуги на платній основі.

Але порядок надання послуг конфіденційного зв'язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям визначає Кабінет Міністрів України.

Послуги конфіденційного зв'язку іншим юридичним та фізичним особам надаються відповідно до законодавства на підставі договору між споживачем та оператором. При цьому законодавство встановлює вимогу до розмежування конфіденційної інформації органів державної влади та органів місцевого самоврядування, інших юридичних та фізичних осіб з використанням криптографічних та/або технічних засобів.

Забезпечення відповідного рівня захисту інформації при наданні послуг конфіденційного зв'язку забезпечується комплексом таких організаційних і технічних заходів:

- шифрування інформації за допомогою вітчизняних засобів криптографічного захисту інформації;
- резервування критичного обладнання та каналів зв'язку,
- цілодобовий контроль за функціонуванням системи;
- блокування розповсюдження комп'ютерних вірусів;
- швидке реагування на можливі спроби несанкціонованого доступу до інформації та ресурсів системи.

Починаючи з 2005 р. у межах цієї системи розвивається Спеціальна мережа стільникового зв'язку НСКЗ, в якій використовуються мобільні термінали, що обладнані системами криптографічного захисту інформації²⁵¹.

В Україні діє також Державна система урядового зв'язку України, яка призначена для передачі інформації, що містить державну таємницю, і використовується виключно органами державної влади.

²⁵¹ Про створення спеціальної мережі стільникового зв'язку Національної системи конфіденційного зв'язку: Розпорядження Кабінету Міністрів України від 24 вересня 2005 р. № 405-р.

9. 6. Державна служба спеціального зв'язку та захисту інформації України

Питання захисту інформації та організації державного управління у цій сфері неодноразово ставали предметом широких дискусій. Певною мірою це пов'язано із незадовільним станом забезпечення прав і свобод громадян, захисту персональних даних, захисту конфіденційної і таємної інформації, порушення щодо яких ставали причинами резонансних подій у політичному, правовому та економічному житті України. Тривалий час основні питання державного управління у сфері захисту інформації та забезпечення органів державної влади і місцевого самоврядування спеціальним зв'язком належали до компетенції Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (ДСТСЗІ СБУ). Але в 2005 р., Президент України ухвалив Указ, яким передбачалося вжиття ряду заходів щодо забезпечення конституційних прав громадян на недоторканність житла, таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції, невтручання в особисте і сімейне життя під час проведення оперативно-технічних заходів та відповідно до ч. 2 ст. 102 Конституції України²⁵².

Одним із цих заходів було визначено необхідність створення центрального органу виконавчої влади із спеціальним статусом основними завданнями якого є: реалізація державної політики у сфері захисту державних інформаційних ресурсів у мережах передачі даних, забезпечення функціонування державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, криптографічного і технічного захисту інформації. Таким органом стала Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку).

Правову основу діяльності Держспецзв'язку було створено із прийняттям Закону України "Про Державну службу спеціального зв'язку та захисту інформації України"²⁵³.

Згідно зі ст. 2 цього Закону, Державна служба спеціального зв'язку та захисту інформації України є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного

²⁵² Про додержання прав людини під час проведення оперативно-технічних заходів: Указ Президента України від 7 листопада 2005 р. № 1556/2005.

²⁵³ Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23 лютого 2006 р. № 3475-IV// Відомості Верховної Ради України. – 2006. – № 30. – Ст. 258.

зв'язку, захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації.

Основними завданнями Держспецзв'язку (ст. 3) є:

- участь у формуванні та реалізації державної політики у сфері захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, криптографічного і технічного захисту інформації;
- забезпечення в установленому порядку урядовим зв'язком Президента України, Голови Верховної Ради України, Прем'єр-Міністра України, інших посадових осіб органів державної влади, органів місцевого самоврядування, органів військового управління, керівників підприємств, установ і організацій у мирний час, в умовах надзвичайного та воєнного стану, а також у разі виникнення надзвичайної ситуації;
- забезпечення функціонування, безпеки та розвитку державної системи урядового зв'язку і Національної системи конфіденційного зв'язку;
- визначення вимог і порядку створення та розвитку систем технічного та криптографічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;
- здійснення державного контролю за станом криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також за дотриманням вимог законодавства у сфері надання послуг електронного цифрового підпису;
- охорона об'єктів, приміщень, систем, мереж, комплексів, засобів урядового і спеціального зв'язку, ключових документів до засобів криптографічного захисту інформації Державної служби спеціального зв'язку та захисту інформації України.

Держспецзв'язок має специфічне потрійне підпорядкування, яке було створено з метою забезпечення ефективного контролю за її діяльністю та запобігання можливим зловживанням у цій сфері.

Так, діяльність Держспецзв'язку спрямовується Кабінетом Міністрів України, який здійснює заходи щодо забезпечення її функціонування. До компетенції Кабміну віднесено також призначення Го-

лови Адміністрації Держспецзв'язку, який здійснює керівництво цією службою.

Водночас Держспецзв'язок підконтрольний Верховній Раді України, а з питань забезпечення національної безпеки України підпорядковується і підконтрольний Президентові України.

Безпосередньо порядок організації діяльності Держспецзв'язку визначається Постановами Кабінету Міністрів України “Питання Адміністрації Державної служби спеціального зв'язку та захисту інформації”²⁵⁴ та “Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації”²⁵⁵.

Кабінет Міністрів України визначає також структуру і штат Держспецзв'язку та її підрозділів²⁵⁶. Структура Дежспецзв'язку є такою:

- Адміністрація Держспецзв'язку – центральний орган виконавчої влади із спеціальним статусом, структурними підрозділами якої є департаменти та управління, відділи й сектори;
- регіональні підрозділи, які забезпечують вирішення покладених на Держспецзв'язку завдань в регіонах України;
- територіальні підрозділи, які вирішують завдання забезпечення функціонування системи урядового зв'язку;
- підрозділи забезпечення (навчальні та медичні підрозділи, науково-дослідні та науково-виробничі установи);
- до сфери державні управління Держспецзв'язку також відносяться державні підприємства, діяльність яких пов'язана із забезпеченням виконання покладених на службу завдань.

Серед підрозділів і установ, що підпорядковані Держспецзв'язку та забезпечують вирішення окремих завдань, що покладені на цю службу, слід назвати:

- *Центр забезпечення урядовим зв'язком Держспецзв'язку у м. Києві та Київській області, що забезпечує функціонування державної системи урядового зв'язку та безпеку інформації в ній безпосередньо у м. Києві;*
- *Державний науково-дослідний інститут спеціального зв'язку та захисту інформації, основними завданнями якого є під-*

²⁵⁴ Питання Адміністрації Державної служби спеціального зв'язку та захисту інформації: Постанова Кабінету міністрів України від 25 травня 2006 р. № 734.

²⁵⁵ Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації: Постанова Кабінету міністрів України від 24 червня 2006 р. № 868.

²⁵⁶ Деякі питання організації діяльності Державної служби спеціального зв'язку та захисту інформації: Постанова Кабінету міністрів України від 24 червня 2006 р. № 869.

готовка пропозицій щодо загальної стратегії розвитку спеціальних інформаційно-телекомунікаційних систем, розробка нормативно-правових актів у цій сфері, проектів створення спеціальних інформаційно-телекомунікаційних систем;

- *Інститут спеціального зв'язку та захисту інформації Національного технічного університету "КПІ"* для підготовки висококваліфікованих фахівців у галузі спеціального зв'язку та захисту інформації для Держспецзв'язку та інших органів виконавчої влади, наукових кадрів, перепідготовки і підвищення кваліфікації інженерних кадрів;

Державне підприємство "Державний центр інформаційної безпеки" – розробка систем криптографічного захисту інформації для органів державної влади;

Державний центр випробувань засобів технічного захисту інформації – забезпечення органів державної влади засобами технічного захисту інформації, перевіреними на відповідність національним стандартам;

Державне підприємство "Українські спеціальні системи" – оператор Національної системи конфіденційного зв'язку, виконує роботи в галузі КЗІ та ТЗІ;

Державне підприємство "Укрінформзв'язок" – оператор Державної системи урядового зв'язку, здійснює виробництво та монтаж систем ТЗІ та апаратури спеціального призначення.

РОЗДІЛ III

ІНФОРМАЦІЙНА ДІЯЛЬНІСТЬ

ГЛАВА 10

ПРАВОВЕ РЕГУЛЮВАННЯ ТЕЛЕКОМУНІКАЦІЙ

Основні моделі правового регулювання інформаційної діяльності. Міжнародно-правові основи регулювання телекомунікацій. Правове регулювання використання радіочастот. Регулювання ринку телекомунікацій. Національна комісія з питань регулювання зв'язку України.

10. 1. Основні моделі правового регулювання інформаційної діяльності

Закон України “Про інформацію” (ст. 12) визначає інформаційну діяльність як сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави. Результатами такої інформаційної діяльності є *інформаційні продукти* як матеріалізований результат цієї діяльності та *інформаційні послуги* як певна сукупність дій з доведенню інформаційної продукції до споживачів.

Законодавство встановлює державні гарантії прав на інформацію та на свободу інформаційної діяльності всім громадянам і юридичним особам у межах їх прав і свобод, функцій і повноважень. Отже, здійснення інформаційної діяльності є важливим механізмом реалізації визначених законодавством прав і свобод у галузі інформації та критерієм оцінювання стану захищеності прав і свобод людини взагалі.

Крім того, нині в умовах глобалізації та інформатизації сфера інформаційної діяльності, яка охоплює такі її основні види, як одержання, використання, поширення та зберігання документованої або оприлюдненої інформації набула величезного економічного, соціального та політичного значення. Сфера інформаційної діяльності багато в чому визначає перспективи подальшого економічного та соціально-політичного розвитку будь-якої сучасної держави.

Таке подвійне значення інформаційної діяльності виявилось в так званій концепції *дуалізму публічного і приватного*, яка спочатку застосовувалася щодо сфери засобів масової інформації, але може і в більш широкому розумінні характеризувати ключові принципи регулювання основних видів інформаційної діяльності взагалі. Згідно з цією концепцією, товари і послуги, що постачаються засобами масової інформації, одночасно є і чимось приватним, і чимось публічним. Оскільки їх споживають для індивідуальних потреб, вони перебувають у приватній власності і використовуються для одержання прибутку, але є також чимось публічним у розумінні, що вони необхідні для процесу демократичної комунікації в суспільному просторі²⁵⁷.

Така подвійна функція основних видів інформаційної діяльності, до яких, зокрема, належать: засоби масової інформації, телекомунікація та зв'язок, видавнича, архівна та бібліотечна справа тощо, зумовлює подвійну специфіку відповідного правового регулювання, яке охоплює відповідну систему дозволів, приписів та обмежень. Так, з одного боку, ці види інформаційної діяльності виконують важливі функції із задоволення інформаційних потреб людини, суспільства і держави. Відповідно правове регулювання публічного аспекту такої діяльності має забезпечувати вирішення комплексу суспільних і державних інтересів. Наприклад, щодо задоволення інформаційних потреб людини та суспільства правове регулювання інформаційної діяльності має забезпечити захист та реалізацію прав і свобод в сфері інформації: свободу слова, право на інформацію, право на повагу до особистого життя тощо. Інформаційна діяльність відіграє важливу роль у державному житті і, отже, інший комплекс правових норм, що регулюють її, має бути спрямований на реалізацію державної інформаційної політики та інформаційне забезпечення діяльності органів публічної влади.

З другого боку, суб'єкти інформаційної діяльності, незалежно від форми власності, діють як суб'єкти господарювання в умовах ринкової економіки та конкуренції. Отже, правове регулювання приватного аспекту інформаційної діяльності має бути спрямоване на створення відповідних економічних умов роботи її суб'єктів, зокрема, на

²⁵⁷ Див.: *McQuail D. Mass Communication Theory: An Intioudction. Third edition. – London: Sage Publications, 1994 – P. 154.*

захист чесної конкуренції, сприяння розвитку, заохочення інвестицій, іноді – на державну підтримку певних напрямів інформаційної діяльності тощо.

Поряд із загальною специфікою правового регулювання інформаційної діяльності, що зумовлена зазначеним дуалізмом публічного і приватного її аспектів, виділяють також три основні моделі правового регулювання окремих видів інформаційної діяльності, що зумовлені специфікою кожного з них²⁵⁸, а саме:

1) модель правового регулювання друкованих ЗМІ (преса, видавнича справа);

2) модель правового регулювання електронних ЗМІ (телебачення і радіомовлення);

3) модель правового регулювання зв'язку (послуги телекомунікації та поштового зв'язку).

Як бачимо, ці моделі розміщені в порядку зростання установлених законодавством обмежень цих видів інформаційної діяльності, яка зумовлена специфікою засобів і способів її здійснення.

Найбільш ліберальною є *модель правового регулювання діяльності друкованих ЗМІ*, асоціюються насамперед із такою категорією, як свобода слова. Це, зокрема, зазначено у нормах ч. 1 ст. 2 Закону України “Про друковані засоби масової інформації (пресу) в Україні”²⁵⁹. Нині свобода діяльності друкованих ЗМІ, свобода слова і вільне вираження у друкованій формі своїх поглядів та переконань гарантуються Конституцією України і, відповідно до цього Закону, означають право кожного громадянина вільно і незалежно шукати, одержувати, фіксувати, зберігати, використовувати та поширювати будь-яку відкриту за режимом доступу інформацію за допомогою друкованих засобів масової інформації.

Свобода діяльності друкованих ЗМІ забезпечується відносно простим порядком їх реєстрації, широким колом фізичних та юридичних осіб, які можуть виступати засновниками друкованих ЗМІ, різноманітністю організаційних форм їх діяльності тощо. Фактично обмеження у сфері діяльності друкованих ЗМІ обмежуються лише питаннями захисту прав та інтересів третіх осіб та забезпеченням дотримання режимів доступу до інформації.

²⁵⁸ Див.: Крос К., Гакет Р. Політична комунікація і висвітлення новин у демократичних суспільствах: перспективи конкуренції. – К.: Основи, 2000 – С. 23 – 26.

²⁵⁹ Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16 листопада 1992 р. // Відомості Верховної Ради України. – 1993. – № 1. – Ст. 1.

Одночасно, Ч. 4 ст. 2 Закону України “Про друковані засоби масової інформації (пресу) в Україні” визначає межі втручання держави в діяльність преси як економічної інституції, яке стосується:

- гарантування економічної самостійності;
- забезпечення економічної підтримки;
- запобігання зловживанню монопольним становищем на ринку з боку видавців і розповсюджувачів друкованої продукції.

Особливості моделі *правового регулювання електронних ЗМІ* зумовлені насамперед специфікою технічних засобів за допомогою яких розповсюджується інформація (мовлення) електронними ЗМІ, а також тим, що здійснення ефірного мовлення потребує використання радіочастотного ресурсу, який за своєю природою є ресурсом обмеженим і потребує впорядкованого користування.

Отже, особливістю моделі правового регулювання електронних ЗМІ є те, що, поряд із властивими для друкованих ЗМІ питаннями захисту та реалізації прав і свобод у сфері інформації та державним регулюванням господарської діяльності, окремого регулювання потребують і технічні аспекти такої діяльності.

Такі технічні аспекти діяльності електронних ЗМІ стосуються, зокрема: виділення радіочастотного спектра, території та обсягу мовлення, технічних стандартів відповідного обладнання та контролю за дотриманням установлених вимог. Відповідно особливістю моделі правового регулювання електронних ЗМІ є ліцензування теле-радіомовлення, яке, згідно з нормами ст. 1 Закону України “Про телебачення і радіомовлення”²⁶⁰ полягає у видачі письмового дозволу, що надає право на створення і використання каналу мовлення та часу мовлення.

Нарешті, в *моделі правового регулювання зв'язку* головною є “ідея рівного, без дискримінації, права на доступ до інформації. Ця модель відображає історичну роль держави в полегшенні комунікації між громадянами за допомогою поштової служби, телефону і телеграфу. Вона пов'язана з універсальним характером комунікаційних служб, які розглядають як суспільні установи, доступні для всіх громадянам. Згідно з цим принципом держава не може заборонити певним категоріям людей користуватися автострадами чи телефонами. Тому режим регулювання зорієнтований не на зміст інформації, а передусім, на ефек-

²⁶⁰ Про телебачення і радіомовлення: Закон України від 21 грудня 1993 р. № 3759-XII // Відомості Верховної Ради України. – 1994. – № 10. – Ст. 43.

тивне будівництво та експлуатацію підприємств із надання цих послуг, модернізацію їх обладнання та інфраструктури”²⁶¹.

Подібна модель реалізована і в національному законодавстві. Наприклад, згідно з нормами ч. 1 ст. 6 Закону України “Про телекомунікації” одним з принципів діяльності у сфері телекомунікацій є “доступ споживачів до загальнодоступних телекомунікаційних послуг, які необхідні їм для задоволення власних потреб, участі в політичному, економічному та громадському житті”²⁶².

Подібна специфіка телекомунікаційних послуг зумовлює відповідні цілі і завдання державного регулювання цієї сфери. Так, за ст. 16 Закону України “Про телекомунікації”, метою державного регулювання у сфері телекомунікацій є:

- максимальне задоволення попиту споживачів на телекомунікаційні послуги;
- створення сприятливих організаційних та економічних умов для залучення інвестицій;
- збільшення обсягів послуг та підвищення їх якості;
- розвиток та модернізація телекомунікаційних мереж;
- урахування інтересів національної безпеки.

Принципові відмінності моделей правового регулювання різних видів інформаційної діяльності зумовили і особливості формування міжнародно-правових стандартів у цій сфері.

В галузі діяльності друкованих ЗМІ міжнародно-правові стандарти стосуються лише основних прав і свобод людини в галузі інформації, щодо яких друковані ЗМІ виступають одним із засобів реалізації. А дозволені міжнародно-правовими актами винятки та обмеження відповідних прав фактично визначають межі, в яких держава може регулювати цей вид інформаційної діяльності.

Стосовно електронних ЗМІ відповідні міжнародно-правові стандарти йдуть дещо далі, що пов’язано з нематеріальним характером носія інформації, що використовуються цими ЗМІ і для якого державні кордони не є перешкодою: Європейська Конвенція про транскордонне телебачення, Декларація керівних принципів використання мовлення через супутники ЮНЕСКО.

²⁶¹ Крос К., Гакет Р. Політична комунікація і висвітлення новин у демократичних суспільствах: перспективи конкуренції. – К. : Основи, 2000 – С. 26.

²⁶² Про телекомунікації: Закон України від 18 листопада 2003 р. № 1280-IV // Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155.

Найбільш врегульованою нормами міжнародного права є сфера телекомунікацій та поштового зв'язку, в якій на міжнародно-правовому рівні вирішуються питання розподілу радіочастот, призначення відповідних кодів країн, взаємодії між операторами та провайдерами послуг зв'язку різних країн. Зокрема, ці питання є предметом діяльності Міжнародного поштового союзу та Міжнародного союзу електрозв'язку. Нарешті, в рамках СОТ діє Генеральна угода з торгівлі послугами (ГАТС), яка забезпечує відкритість національних ринків країн-учасниць щодо послуг з-за кордону, зокрема і послуг телекомунікацій.

10. 2. Міжнародно-правові основи регулювання телекомунікацій

Розвиток національної системи телекомунікацій неможливий без інтеграції у глобальні телекомунікаційні мережі та ефективної міжнародної співпраці в цій сфері. За ст. 72 Закону України “Про телекомунікації” основними напрямками міжнародної співпраці у сфері телекомунікацій є:

- укладання міжнародних договорів;
- участь у роботі міжнародних організацій;
- участь у реалізації міжнародних проєктів, пов'язаних із створенням глобальної і регіональних телекомунікаційних мереж з урахуванням інтересів національної безпеки України;
- гармонізація стандартів, норм і правил з міжнародними стандартами, рекомендаціями, нормами і правилами, які стосуються вимог до технічних засобів і телекомунікаційних мереж, взаємодії операторів телекомунікацій, використання обмежених ресурсів, якості і видів телекомунікаційних послуг.

Основні заходи міжнародної співпраці у сфері телекомунікацій Україна здійснює у межах Міжнародного союзу електрозв'язку, членом якого вона є з 1994 р., та в рамках європейських і регіональних організацій зв'язку і телекомунікацій. Крім того, в рамках Світової організації торгівлі (СОТ) питання регулювання ринку телекомунікацій розглядаються в Раді торгівлі послугами СОТ. Представлення інтересів України у цих міжнародних організаціях покладено на Адміністрацію зв'язку та радіочастот України, функції якої виконує Міністерство транспорту і зв'язку України.

Правовою основою діяльності *Міжнародного союзу електрозв'язку* є такі міжнародно-правові акти, як *Конвенція Міжнародного союзу електрозв'язку* та *Статут Міжнародного союзу електрозв'язку*, які були підписані Україною 22 грудня 1994 р. і ратифіковані в липні 1994 р.²⁶³.

Керівні органи Міжнародного союзу електрозв'язку складаються з Повноважної Конференції, яка є вищим органом Союзу, і Ради, яка діє від імені Повноважної Конференції та виконує її функції у періоди між проведенням засідань останньої та всесвітніх конференцій з міжнародного електрозв'язку. Функції виконавчого органу Союзу виконує Генеральний секретаріат.

До структури Міжнародного союзу електрозв'язку належать також:

- Сектор радіозв'язку, в т. ч. всесвітні і регіональні конференції радіозв'язку, асамблеї радіозв'язку і Радіорегламентарний комітет;
- Сектор стандартизації електрозв'язку, у т. ч. всесвітні й регіональні конференції із стандартизації електрозв'язку;
- Сектор розвитку електрозв'язку, у т. ч. всесвітні і регіональні конференції з розвитку електрозв'язку;

Основними цілями діяльності Міжнародного союзу електрозв'язку, що визначені ст. 1 його Статуту, є:

- розподіл радіочастотного спектра, виділення радіочастот і реєстрація присвоєних радіочастот та відповідних позицій на орбіті геостационарних супутників так, щоб уникнути шкідливих перешкод між радіостанціями різних країн;
- координація зусиль, спрямованих на усунення шкідливих перешкод між радіостанціями різних країн і на поліпшення використання спектра радіочастот і орбіт геостационарних супутників для служб радіозв'язку;
- полегшення міжнародної стандартизації електрозв'язку із задовільною якістю обслуговування.

Для виконання зазначених цілей Союз, окремі його підрозділи або відповідні міжнародні конференції можуть ухвалювати рішення, вносити зміни до чинних міжнародних угод та регламентів і заохочувати країни-члени до підписання нових міжнародних угод.

У Статуті й Конвенції Міжнародного союзу електрозв'язку визначено правовий статус і порядок діяльності цієї організації, права та обов'язки її членів.

²⁶³ Про ратифікацію Статуту і Конвенції Міжнародного союзу електрозв'язку: Закон України від 15 липня 1994 р. № 116/94-ВР // Відомості Верховної Ради України. – 1994. – № 33. – Ст. 306.

Безпосередньо питання електрозв'язку (розподіл радіочастотного ресурсу, відповідні заходи з присвоєння і реєстрації радіочастот, усунення перешкод, взаємодію між операторами телекомунікацій різних країн та пов'язані з цим технічні стандарти) визначаються так званими Адміністративними регламентами:

- Регламентом міжнародного електрозв'язку;
- Регламентом радіозв'язку.

За правилами, що визначені цими регламентами, створюються багатосторонні регіональні та двосторонні міжнародні угоди й національні нормативно-правові акти у сфері зв'язку й телекомунікацій. Зокрема, згідно з умовним територіально-адміністративним розподілом Міжнародного союзу електрозв'язку, Україна належить до Району 1.

Так, Україна є учасницею Угоди про створення Регіональної співдружності в галузі зв'язку, (РСЗ) підписаної в рамках СНД²⁶⁴. Регіональна співдружність в галузі зв'язку будує свої відносини з Міжнародним союзом електрозв'язку та Всесвітнім поштовим союзом на правах регіонального органу. Згідно зі Статутом цієї організації, її завданнями є:

- розширення взаємовигідних відносин між Адміністраціями зв'язку – учасниками РСЗ, гармонізація розвитку зв'язку;
- спільне вивчення пропозицій, що подаються на з'їзди й конференції міжнародних організацій зв'язку та в їхні робочі органи, підготовка рекомендацій, що виражають спільний інтерес учасників РСЗ;
- розроблення рекомендацій щодо принципів взаєморозрахунків за послуги зв'язку між адміністраціями зв'язку – учасниками РСЗ, а також між ними та іншими державами.
- координація діяльності адміністрацій зв'язку – учасників РСЗ з питань електромагнітної сумісності, раціонального використання спектра радіочастот і орбіти геостационарних супутників зв'язку й віщання.

Ще один аспект міжнародно-правового регулювання телекомунікацій – міжнародна торгівля послугами, зокрема, й телекомунікаційними, основні принципи якої визначаються нормами Генеральної угоди з торгівлі послугами 1994 р. (ГАТС), яка є невід'ємною частиною багатосторонніх торговельних угод СОТ (Додаток 1В до Угоди про заснування Світової Організації Торгівлі)²⁶⁵.

²⁶⁴ Соглашение о создании Регионального содружества в области связи. Москва, 17 декабря 1991 г.

²⁶⁵ Генеральна угода з торгівлі послугами 1994 р. / Україна і Світова організація торгівлі: 36. офіц. док. – К., 2002.

Основним завданням ГАТС є укладення багатостороннього зведення принципів і правил торгівлі послугами з метою розширення такої торгівлі на умовах гласності і подальшої лібералізації. Положення цієї угоди стосуються заходів країн-членів, що впливають на торгівлю послугами. ГАТС запроваджує триступеневу систему регулювання таких заходів:

- загальні правила і принципи, встановлені безпосередньо нормами ГАТС, які застосовуються всіма країнами-учасницями при проведенні заходів регулюванні будь-яких видів послуг;
- додатки до ГАТС стосовно телекомунікацій та переговорів щодо стосовно основних телекомунікацій, якими встановлюються додаткові правила, в торгівлі телекомунікаційними послугами;
- специфічні (індивідуальні) зобов'язання щодо доступу на національний ринок, які беруть на себе країни-члени стосовно конкретних секторів послуг згідно відповідно до підписаних ними списків поступок.

Основними загальними правилами ГАТС є *режим найбільшого сприяння та національний режим* заходів з регулювання торгівлі телекомунікаційними послугами.

Режим найбільшого сприяння в контексті ГАТС (ст. II) полягає в тому, що в рамках дії положень ГАТС кожен її член повинен надати негайно і безумовно для послуг і постачальників послуг будь-якого іншого члена угоди режим, не менш сприятливий, аніж той, який він надає для таких самих послуг або постачальників послуг будь-якої іншої країни.

Національний режим у цьому разі (ст. XVII ГАТС) передбачає зобов'язання країн членів у секторах, що визначені в їхніх специфічних зобов'язаннях, надавати послугам і постачальникам послуг будь-якого іншого члена щодо всіх заходів, які стосуються поставки послуг, режим, не менш сприятливий, за той, який він надає таким самим своїм послугам або постачальникам послуг.

Специфічні зобов'язання країн-членів ГАТС поділяються на “горизонтальні”, що стосуються всіх видів послуг, і “секторальні” – щодо конкретних секторів послуг. Секторальні зобов'язання відповідають на Класифікаторі секторів послуг, прийнятому свого часу в рамках ООН²⁶⁶, якій налічує 12 секторів і 155 підсекторів, в тому числі сектор послуг засобів зв'язку, який включає 24 підсектори.

²⁶⁶ Provisional Central Product Classification. Statistical Office of the United Nations. – Statistical Papers. Series M. –No. 77. – New York, 1991.

У специфічних зобов'язаннях щодо відповідного виду послуг зазначено:

- термін “нічого” (*none*), що означає відсутність обмежувальних заходів щодо доступу на ринок послуг;
- термін “незв’язаний” (*unbound*), який означає, що держава може застосовувати будь-які обмеження на власний розсуд;
- вичерпний перелік обмежувальних заходів, що застосовуються щодо доступу на ринок в певному секторі послуг.

Питання торгівлі послугами, врегульовані ГАТС, є предметом діяльності Ради з торгівлі товарами СОТ, а спори щодо застосування тих чи інших положень відповідних угод вирішуються в рамках Механізму врегулювання спорів СОТ.

10. 3. Правове регулювання використання радіочастот.

Одним із важливих аспектів регулювання діяльності засобів телекомунікації та електронних засобів масової інформації є розподіл і присвоєння радіочастот та контроль за використанням радіочастотного ресурсу.

Згідно зі ст. 1 Закону “Про радіочастотний ресурс України”²⁶⁷, *радіочастотний ресурс – це частина радіочастотного спектра, придатна для передавання та приймання електромагнітної енергії радіоелектронними засобами, яку можна використовувати на території України та за її межами відповідно до законів України та міжнародного права, а також на виділених для України частотно-орбітальних позиціях.*

Надання права на користування радіочастотним ресурсом реалізується за допомогою тріступеневої процедури.

На першому етапі здійснюється *розподіл смуг радіочастот*, тобто регламентування відповідним записом у Національній таблиці розподілу смуг радіочастот України використання певної заданої смуги радіочастот однією чи кількома радіослужбами.

На другому, відповідно до розподілу смуг радіочастот, здійснюється *виділення радіочастот* – надання відповідним записом у Плані використання радіочастотного ресурсу України права використовувати

²⁶⁷ Про радіочастотний ресурс України: Закон від 1 червня 2000 р. № 1770-III // Відомості Верховної Ради України. – 2000. – № 36. – Ст. 298.

вати певні смуги радіочастот для застосування в Україні визначених цим Планом радіотехнологій.

Нарешті, третім етапом є *присвоєння смуг та номіналів радіочастот* – реєстрація дозволу на експлуатацію радіоелектронних засобів і випромінювальних пристроїв у реєстрі присвоєнь смуг, номіналів радіочастот з визначенням смуги, номіналу радіочастот, параметрів випромінювання та умов експлуатації конкретного радіоелектронного засобу.

Згідно зі ст. 5 Закону “Про радіочастотний ресурс України”, всі користувачі радіочастотного ресурсу України залежно від напрямів його використання поділяються на дві категорії: спеціальні користувачі та загальні користувачі.

До *спеціальних користувачів* радіочастотного ресурсу України належать:

- підрозділи і організації Міністерства оборони України, Служби безпеки України, Служби зовнішньої розвідки України, Державної служби спеціального зв’язку та захисту інформації України, Міністерства внутрішніх справ України, Міністерства з надзвичайних ситуацій України та ліквідації наслідків Чорнобильської катастрофи, Адміністрації Державної прикордонної служби України, Управління державної охорони, Державного департаменту з питань виконання покарань, Державної податкової адміністрації України (у частині застосування радіоелектронних засобів податковою міліцією), якщо їх діяльність пов’язана з використанням радіоелектронних засобів виключно для виконання функціональних обов’язків і за умови їх фінансування виключно за рахунок Державного бюджету України;
- Міністерства транспорту України в частині застосування радіоелектронних засобів об’єднаної цивільно-військової системи організації повітряного руху України та забезпечення польотів і в частині застосування радіоелектронних засобів Державною спеціальною службою транспорту.

Всі інші користувачі радіочастотного ресурсу належать до категорії *загальних користувачів*, які поділяються на три групи:

- суб’єкти господарювання, які користуються радіочастотним ресурсом України для надання телекомунікаційних послуг, за винятком розповсюдження телерадіопрограм;

- суб'єкти господарювання, які здійснюють розповсюдження телерадіопрограм із застосуванням власних або орендованих радіоелектронних засобів;
- технологічні користувачі і радіоаматори – юридичні чи фізичні особи, які користуються радіочастотним ресурсом України без надання телекомунікаційних послуг.

За використання радіочастотного ресурсу стягується плата, яка розраховується відповідно до ставок, затверджених Кабінетом Міністрів України, щомісячно за кожен 1 МГц радіочастот у кожному окремому регіоні.

Органами, що безпосередньо здійснюють управління та контроль за користуванням радіочастотним ресурсом України, є:

- *Генеральний штаб Збройних Сил України*, який здійснює виділення радіочастот, надання дозволів на користування радіочастотним ресурсом та контроль за дотриманням законодавства в цій галузі спеціальними користувачами;
- *Національна комісія з питань регулювання зв'язку (НКРЗ), Державна інспекція зв'язку (ДІЗ) та Український державний центр радіочастот (УДЦР)*, які виконують функції щодо виділення радіочастот, ліцензування та контролю за діяльністю загальних користувачів.

Основними нормативно-правовими актами, що безпосередньо визначають розподіл радіочастотного ресурсу, є Національна таблиця розподілу радіочастот та План використання радіочастотного ресурсу України.

Національна таблиця розподілу смуг радіочастот України є нормативно-правовим актом що регламентує розподіл смуг радіочастот радіослужбам в Україні та визначає смуги радіочастот спеціального й загального користування.

Цю Таблицю розробляє Міністерство транспорту і зв'язку України за участю Національної комісії регулювання зв'язку (НКРЗ), Національної ради України з питань телебачення і радіомовлення, Генерального штабу Збройних Сил України, інших заінтересованих органів державної влади на основі Регламенту радіозв'язку Міжнародного союзу електрозв'язку та затверджує Кабінет Міністрів України²⁶⁸.

²⁶⁸ Про затвердження Національної таблиці розподілу смуг радіочастот України: Постанова Кабінету Міністрів України від 15 грудня 2005 р. № 1208.

Національна таблиця розподілу смуг радіочастот України складається з трьох граф:

У *графі першій* наведено дані про розподіл смуг радіочастот між радіослужбами і номери приміток згідно з Регламентом радіозв'язку Міжнародного союзу електрозв'язку.

У *графі другій* визначено розподіл смуг радіочастот між радіослужбами в Україні і номери приміток до нього, що починаються з літери “У”, зміст яких викладено в кінці Таблиці.

У *графі третій* Таблиці вказано призначення смуг радіочастот в Україні: загального користування (ЗК) або спеціального користування (СК).

Радіочастотний ресурс України використовується за *Планом використання радіочастотного ресурсу України*, який складають відповідно до Національної таблиці розподілу радіочастот з урахуванням рекомендацій Міжнародного союзу електрозв'язку, Європейської конференції адміністрацій пошт та електрозв'язку (СЕРТ) та пропозицій зацікавлених органів державної влади, громадських організацій і суб'єктів господарської діяльності – користувачів радіочастотного ресурсу України.

Цей план є постійнодіючим нормативно-правовим актом, що затверджується Кабінетом Міністрів України²⁶⁹. Він складається з двох розділів і додатків. У Розділі I наведено перелік радіотехнологій, які використовуються в Україні, з визначенням смуг радіочастот та служб радіозв'язку, а також строки припинення їх використання. Відповідні дані подано у вигляді таблиці, що складається з восьми граф:

21. Цифровий стільниковий радіозв'язок GSM – 1800	рухома	Стільниковий радіозв'язок	ESC – 1800	ГОСТ	ERC/DEC (95) 03	1710 – 1785 МГц 1805 – 1880 МГц	Л01, Д01
---	--------	---------------------------	------------	------	-----------------	---------------------------------	----------

У відповідних графах, зокрема, зазначено:

перша – радіотехнології, що використовуються радіослужбами в Україні;

друга – радіослужби, котрі використовують ці радіотехнології;

третья – вид радіозв'язку, якому відповідає та чи інша радіотехнологія;

²⁶⁹ Про затвердження Плану використання радіочастотного ресурсу України: Постанова Кабінету Міністрів України від 9 червня 2006 р. № 815.

четверта і п'ята – базові національні стандарти;

шоста – положення: 1) Міжнародного союзу електрозв'язку, 2) Європейської конференції адміністрацій пошт та електрозв'язку (СЕПТ), 3) Європейської комісії з комунікацій (ЄКК), 4) міжнародні угоди, в яких визначаються умови використання радіочастотного ресурсу щодо забезпечення електромагнітної сумісності (ЕМС) радіоелектронних засобів (РЕЗ);

сьома – смуги або номінали радіочастот, виділені для використання в радіотехнологіях;

восьма – особливості застосування радіотехнологій в Україні та умовні позначення ліцензій і дозволів, що дають право на користування радіочастотним ресурсом.

У плані може бути визначений строк припинення використання радіочастоти відповідною службою.

У Розділі II Плану використання радіочастотного ресурсу України наведено перелік перспективних для впровадження в Україні радіотехнологій із визначенням радіослужб, які планують їх використання, смуг радіочастот, а також строки впровадження радіотехнологій.

Присвоюючи конкретним користувачам відповідні смуги та номінали радіочастот, права на їх використання визначають такими документами, як: ліцензія на користування радіочастотним ресурсом та дозвіл на експлуатацію радіоелектронних засобів.

Ліцензії на користування радіочастотним ресурсом України видаються *Національною комісією з регулювання зв'язку України* одночасно з видачею ліцензії на вид діяльності у сфері телекомунікацій, що передбачає користування радіочастотним ресурсом України.

Присвоєння радіочастот у смугах радіочастот, виділених для телерадіомовлення, здійснюється на підставі ліцензії на мовлення, яка видається телерадіомовним організаціям *Національною радою з питань телебачення і радіомовлення України*.

Ліцензія на користування радіочастотним ресурсом України – це документ, який засвідчує право суб'єкта господарювання на користування радіочастотним ресурсом України. При цьому у ліцензії обов'язково зазначають:

- термін, протягом якого дозволяється користування радіочастотним ресурсом (як правило, не менше 5 років);
- конкретні регіони, в яких ліцензіат має право на користування радіочастотним ресурсом;

- конкретні смуги та номінали радіочастот, які виділяються в користування;
- інші ліцензійні умови, що підлягають виконанню.

Ліцензія на право користування радіочастотним ресурсом може передбачати:

- 1) виключне право на користування визначеним у ній радіочастотним ресурсом у межах зазначених регіонів
- 2) використання її в межах одного регіону кількома користувачами за умови забезпечення електромагнітної сумісності радіоелектронних засобів.

Експлуатація конкретних радіоелектронних засобів можлива лише за наявності *дозволу на експлуатацію радіоелектронних засобів*, який видає Український державний центр радіочастот (УДЦР) для загальних користувачів або Генеральний штаб ЗСУ для спеціальних користувачів. Відповідний дозвіл видається на підставі *висновку щодо електромагнітної сумісності*, який також надається зазначеними органами.

Дозволи на експлуатацію радіоелектронних засобів можуть надаватися:

- на кожний радіоелектронний засіб, установлений у місці з конкретними географічними координатами;
- на кожний радіоелектронний засіб для використання на зазначеній у дозволі території.

Інколи в дозволі можуть бути визначені умови електромагнітної сумісності з іншими користувачами.

10. 4. Регулювання ринку телекомунікацій

Закон України “Про телекомунікації” (ст. 1) визначає *телекомунікації, або електрозв’язок, як передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних або інших електромагнітних системах.*

Суб’єктами інформаційної діяльності в галузі телекомунікацій є оператори та провайдери телекомунікацій.

Оператор телекомунікацій це – суб’єкт господарювання, який має право на діяльність у сфері телекомунікацій із правом на технічне обслуговування та експлуатацію телекомунікаційних мереж;

Провайдер телекомунікацій – суб’єкт господарювання, який має право на діяльність у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв’язку;

Органом регулювання у сфері телекомунікацій, за ст. 17 Закону України “Про телекомунікації” визначає Національна комісія з питань регулювання зв’язку України. Основними засобами державного регулювання у сфері телекомунікацій є: *нагляд за ринком телекомунікацій, ліцензування діяльності у сфері телекомунікацій, визначення принципів взаємоз’єднання телекомунікаційних мереж, визначення основ розвитку та надання загальнодоступних телекомунікаційних послуг, регулювання тарифів і розподіл номерного ресурсу.*

Нагляд за ринком телекомунікацій, відповідно до ст. 19 Закону України “Про телекомунікації”, здійснюється шляхом:

- контролю за якістю телекомунікаційних послуг;
- перевірки додержання ліцензійних умов операторами, провайдерами телекомунікацій;
- контролю за додержанням суб’єктами ринку телекомунікацій законодавства, стандартів та інших нормативних актів у сфері телекомунікацій.

Ліцензування у сфері телекомунікацій передбачає такі дії НКРЗ, як: видача, переоформлення, продовження терміну дії, визнання недійсними, анулювання ліцензій, видача копій і дублікатів ліцензій, ведення ліцензійних справ та ліцензійних реєстрів, контроль за додержанням ліцензійних умов, видача розпоряджень про усунення порушень ліцензійних умов;

Згідно зі ст. 43 Закону України “Про телекомунікації”, ліцензуванню підлягають такі види діяльності у сфері телекомунікацій:

- надання послуг фіксованого телефонного зв’язку з правом технічного обслуговування та експлуатації телекомунікаційних мереж і надання в користування каналів електрозв’язку;
- надання послуг фіксованого телефонного зв’язку з використанням безпроводового доступу до телекомунікаційної мережі з правом технічного обслуговування і надання в користування каналів електрозв’язку;
- надання послуг рухомого (мобільного) телефонного зв’язку з правом технічного обслуговування та експлуатації теле-

комунікаційних мереж і надання в користування каналів електрозв'язку;

- надання послуг з технічного обслуговування і експлуатації телекомунікаційних мереж, мереж ефірного теле- та радіомовлення, проводового радіомовлення та телемереж;
- надання в користування каналів електрозв'язку.

У ліцензії на здійснення діяльності у сфері комунікацій зазначається конкретний вид діяльності, строк дії ліцензії, який установлюється НКРЗ, але не менш ніж п'ять років, та зазначається територія, на якій здійснюється діяльність у сфері телекомунікацій на підставі цієї ліцензії.

Ефективне функціонування всієї системи електричного зв'язку України неможливо без взаємоз'єднання телекомунікаційних мереж, що належать різним операторам телекомунікацій. Під *взаємоз'єднанням телекомунікаційних мереж* розуміють установлення фізичного та/або логічного з'єднання між різними телекомунікаційними мережами з метою забезпечення можливості споживачам безпосередньо або опосередковано обмінюватись інформацією.

Запобігання зловживанням окремих операторів телекомунікацій та забезпечення функціонування всієї системи зв'язку одним із напрямків державного регулювання ринку телекомунікацій є *визначення принципів взаємоз'єднання телекомунікаційних мереж*.

За ст. 57 Закону України “Про телекомунікації”, технічні, організаційні та економічні умови взаємоз'єднання телекомунікаційних мереж операторів телекомунікацій, а також розрахункові такси за доступ до цих мереж мають бути предметом договору між операторами телекомунікацій, що взаємопідключаються.

НКРЗ наділена широкими повноваженнями щодо контролю за укладанням договорів між операторами телекомунікацій у цій сфері, який вона здійснює з метою:

- забезпечення ефективної конкуренції;
- забезпечення умов, які є недискримінаційними, чесними і прийнятними для обох сторін договору;
- забезпечення умов, які є корисними для споживачів.

Згідно із законодавством НКРЗ, за зверненням будь-якої із сторін, повинна втручатись у відносини операторів телекомунікацій при укладанні договорів про взаємоз'єднання їх телекомунікаційних ме-

реж та протягом місяця з дня звернення зобов'язана прийняти відповідне рішення.

Рішення НКРЗ з питань, що виникають між операторами телекомунікацій при укладанні договору про взаємоз'єднання їх телекомунікаційних мереж, є обов'язковим для виконання операторами телекомунікацій і може бути скасоване лише за рішенням суду.

Держава визначає основи розвитку та надання загальнодоступних телекомунікаційних послуг, загальна мета яких полягає у наданні громадянам України, за регульованими державою тарифами, можливості задовольняти власні потреби в телекомунікаційних послугах, визначених цим Законом, повноцінно брати участь у політичному, економічному та громадському житті суспільства.

До загальнодоступних телекомунікаційних послуг (ст. 62 Закону України “Про телекомунікації”) належать:

- підключення кінцевого обладнання споживача до телекомунікаційних мереж загального користування (універсальний доступ);
- послуги фіксованого телефонного зв'язку в межах зони нумерації (місцевий телефонний зв'язок);
- виклик служб екстреної допомоги;
- послуги довідкових служб і зв'язку за допомогою таксофонів.

Загальнодоступними телекомунікаційними послугами є:

- дзвінки з телекомунікаційних мереж фіксованого телефонного на телекомунікаційні мережі рухомого (мобільного) зв'язку;
- послуги, що надаються з використанням безпроводового доступу.

Ще один напрям регулювання ринку телекомунікацій – *регулювання тарифів*. За загальним правилом тарифи на телекомунікаційні послуги встановлюють оператори, провайдери телекомунікацій самостійно, але при цьому вони повинні враховувати встановлені законодавством принципи регулювання тарифів, зокрема:

- базування розрахунків тарифів на собівартості цих послуг з урахуванням отримання прибутку;
- недопущення встановлення демпінгових або дискримінаційних цін з боку окремих операторів, провайдерів телекомунікацій;
- стягнення почасової плати за фактичний час отримання споживачем телекомунікаційних послуг.

Одночасно, за нормами ч. 2 ст. 66 Закону України “Про телекомунікації” державному регулюванню шляхом установлення граничних або фіксованих тарифів підлягають:

- тарифи на загальнодоступні послуги;
- тарифи на надання в користування каналів електрозв'язку операторів телекомунікацій, які посідають монопольне (домінуюче) становище на ринку цих послуг.

Нарешті, важливим аспектом регулювання ринку телекомунікацій є *формування та розподіл номерного ресурсу*. Відповідно до норм Закону України “Про телекомунікації” (статті 69, 70) формування та розподіл номерного ресурсу здійснюються на основі того, що номерний ресурс є технічно обмеженим.

Розроблення та реалізацію технічної політики у формуванні номерного ресурсу здійснює Мінтрансв'язку, затверджуючи Національний план нумерації України²⁷⁰, що розробляється згідно з міжнародними вимогами.

Відповідно до Національного плану нумерації, НКРЗ здійснює розподіл, присвоєння, облік номерного ресурсу, видачу та скасування дозволів, нагляд за його використанням.

Номерний ресурс надається оператору телекомунікацій на термін дії відповідної ліцензії для використання без права передачі іншим особам, крім випадків вторинного розподілу відповідно до законодавства, на підставі дозволу, що надається НКРЗ.

10. 5. Національна комісія з питань регулювання зв'язку України.

Основним органом державної влади, що здійснює регулювання у сфері телекомунікацій, користування радіочастотним ресурсом та надання послуг поштового зв'язку, є Національна комісія з питань регулювання зв'язку України. Згідно зі ст. 17 Закону України “Про телекомунікації”, НКРЗ є центральним органом виконавчої влади із спеціальним статусом, який є підконтрольний Президенту України та діє на підставі Положення²⁷¹, затвердженого Кабінетом Міністрів України.

Основними завданнями НКРЗ є такі:

- проведення єдиної державної політики регулювання в галузі зв'язку;

²⁷⁰ Про затвердження Національного плану нумерації України: Наказ Міністерства транспорту і зв'язку України від 23 листопада 2006 р. № 1105.

²⁷¹ Про затвердження Положення про Національну комісію з питань регулювання зв'язку України : Постанова Кабінету Міністрів України від 25 липня 2007 р. № 971.

- здійснення державного регулювання та нагляду в галузі зв'язку з метою максимального задоволення попиту споживачів на послуги зв'язку, створення сприятливих умов для залучення інвестицій, збільшення обсягів послуг та підвищення їх якості, розвитку та модернізації мереж зв'язку з урахуванням інтересів національної безпеки;
- забезпечення ефективного користування радіочастотним ресурсом України і функціонування ринку телекомунікаційних послуг та послуг поштового зв'язку на основі збалансування інтересів суспільства, операторів та користувачів цих послуг;
- сприяння розвитку конкуренції та підприємництва, забезпечення однакових умов діяльності суб'єктів усіх форм власності, вдосконалення механізмів регулювання ринкових відносин у галузі зв'язку.

Комісія складається із голови та семи членів, яких призначає на посади та припиняє їх повноваження на цих посадах Кабінет Міністрів України.

Голова і члени Комісії призначаються на посаду строком на п'ять років. Ні голова, ні жоден член Комісії не можуть обіймати посаду більше ніж десять років сумарно.

Законодавством визначені вимоги до голови і членів Комісії: вік – не старше 65 років, вища освіта, наявність практичного й управлінського досвіду, стаж роботи в галузі зв'язку не менше чотирьох років.

Установлено також вимоги до несумісності роботи у складі НКРЗ з певними видами діяльності. Так, голова і члени Комісії не можуть бути власниками корпоративних прав операторів телекомунікацій і поштового зв'язку, виробників телекомунікаційного обладнання, діяльність яких відповідно до закону регулюється Комісією, отримувати від них фінансову або матеріальну винагороду та допомогу чи обіймати будь-яку посаду, в тому числі на громадських засадах.

Формою роботи НКРЗ є засідання, які вона уповноважена проводити за наявності щонайменше п'яти її членів. Засідання проводяться у формі відкритих або закритих слухань. У разі розгляду питань, що мають важливе суспільне значення, засідання проводяться у формі відкритих слухань, у яких мають право брати участь суб'єкти ринку телекомунікацій та ринку послуг поштового зв'язку і громадські організації в установленому Комісією порядку. За результатами засідань ухвалюються рішення.

Безпосередньо порядок роботи цієї Комісії визначається Регламентом національної комісії регулювання зв'язку України²⁷², за нормами якого (п. 4. 19) на засіданнях НКРЗ, відповідно до її компетенції та вимог законодавства, розглядаються такі питання:

- затвердження нормативно-правових актів та нормативних актів із питань, що належать до компетенції НКРЗ, затвердження змін до Регламенту НКРЗ;
- ліцензування та реєстрація у сферах надання телекомунікаційних послуг, послуг поштового зв'язку, а також користування радіочастотним ресурсом України;
- розподіл і присвоєння номерного ресурсу, видача і скасування дозволів на використання номерного ресурсу;
- застосування в установленому законодавством порядку санкцій за порушення законодавства про телекомунікації до суб'єктів ринку телекомунікацій, послуг поштового зв'язку та користувачів радіочастотного ресурсу;
- тарифного регулювання у сфері телекомунікацій, на послуги поштового зв'язку, установлення розрахункових такс за доступ до телекомунікаційних мереж операторів телекомунікацій, плати за видачу дозволів на експлуатацію;
- досудове вирішення спорів між операторами, провайдерами телекомунікацій щодо взаємоз'єднання телекомунікаційних мереж;
- затвердження Статуту Українського державного центру радіочастот та Положення про Державну інспекцію зв'язку;

Частина функцій НКРЗ виконується через підпорядковані йому Державну інспекцію зв'язку (ДІЗ) та державне підприємство “Український державний центр радіочастот” (УДЦР).

Державна інспекція зв'язку є структурним підрозділом НКРЗ. Її компетенція визначається нормами Закону України “Про радіочастотний ресурс” (ст. 15) та Закону України “Про телекомунікації”. Безпосередньо порядок діяльності ДІЗ визначається Положенням про Державну інспекцію зв'язку, затверджене рішенням НКРЗ²⁷³.

До основних повноважень ДІЗ, згідно із Законом “Про радіочастотний ресурс України”, належать:

²⁷² Регламент Національної комісії з питань регулювання зв'язку України. Затверджено Рішенням Національної комісії регулювання зв'язку України від 17 травня 2005 р. № 1.

²⁷³ Про затвердження Положення про Державну інспекцію зв'язку: Рішення Національної комісії з питань регулювання зв'язку України від 2 серпня 2007 р. № 875.

- здійснення державного нагляду за користуванням радіочастотним ресурсом України та запобігання правопорушенням при користуванні ним у смугах радіочастот загального користування;
- підготовка матеріалів для прийняття НКРЗ рішень за наслідками перевірок;
- притягнення в установленому законом порядку до адміністративної відповідальності осіб, винних у порушенні законодавства про радіочастотний ресурс України.
- здійснення державного нагляду за ринком телекомунікацій

Крім того, відповідно до Порядку здійснення державного нагляду за ринком телекомунікацій, затвердженого рішенням НКРЗ, на Державну інспекцію зв'язку покладено функції здійснення державного нагляду за ринком телекомунікацій²⁷⁴.

ДІЗ очолює начальник, який має трьох заступників, у тому числі одного першого.

Нині до структури центрального апарату ДІЗ входять: Управління державного нагляду, Управління планування та організації державного нагляду, Управління захисту прав споживачів та контролю якості послуг, Управління забезпечення діяльності ДІЗ, відділи кадрового забезпечення та управління персоналом, бухгалтерського обліку та звітності, юридичний.

Крім того, свої функції ДІЗ виконує через свої територіальні підрозділи: Центральне, Південне, Північне, Східне, Західне управління та Кримський відділ.

За ст. 16 Закону “Про радіочастотний ресурс України” *державне підприємство “Український державний центр радіочастот” (УДЦР)* належить до сфери управління НКРЗ і здійснює свою діяльність на підставі статуту, який затверджується НКРЗ. Повноваження УДЦР поширюються на користувачів радіочастотного ресурсу України, які діють у смугах радіочастот загального користування.

Основні види діяльності УДЦР такі:

- присвоєння радіочастот, призначення позивних сигналів радіоелектронним засобам (РЕЗ) у смугах радіочастот загального користування;
- ведення реєстру присвоєнь радіочастот;

²⁷⁴ Рішення Національної комісії з питань регулювання зв'язку України “Про затвердження Порядку здійснення державного нагляду за ринком телекомунікацій” від 27 жовтня 2006 р. № 426.

- реєстрація присвоєнь радіочастот РЕЗ України у Міжнародному союзі електрозв'язку та міжнародну координацію присвоєнь радіочастот РЕЗ України й інших країн у прикордонних зонах;
- видача дозволів на експлуатацію, ввезення з-за кордону і реалізацію РЕЗ та випромінювальних пристроїв;
- здійснення радіочастотного моніторингу використання радіочастотного ресурсу України у смугах радіочастот загального користування;
- здійснення технічної експертизи на відповідність параметрам електромагнітної сумісності і вимогам державних стандартів РЕЗ, височастотних пристроїв, об'єктів і споруд зв'язку перед їх упровадженням;
- проведення робіт із підтвердження відповідності (в тому числі із сертифікації), а також сертифікаційні випробування, приймальні випробування РЕЗ і випромінювальних пристроїв на місці експлуатації.

УДЦР здійснює роботи і надає послуги на договірних засадах. Перелік робіт і послуг, які виконує УДЦР, а також тарифи на них затверджуються НКРЗ у встановленому порядку.

ГЛАВА 11

ПРАВОВЕ РЕГУЛЮВАННЯ ФУНКЦІОНУВАННЯ МЕРЕЖІ ІНТЕРНЕТ

Основні поняття і принципи функціонування Інтернет, визначені національним законодавством. Суб'єкти і об'єкти правовідносин, що виникають стосовно функціонування Інтернет. Правові основи адміністрування домену "UA". Декларація Ради Європи "Про свободу спілкування в Інтернет". Національна програма інформатизації. Електронні документи та електронний документообіг. Концепція створення "електронного уряду". Національний реєстр електронних інформаційних ресурсів.

11. 1. Основні поняття і принципи функціонування Інтернет, визначені національним законодавством.

Розглядаючи правовий режим інформаційних ресурсів і доступу до них, варто зважити на те, що нині найбільш складною є проблема правового регулювання відповідних аспектів функціонування глобальної світової мережі Інтернет. Труднощі починалися навіть від того, що протягом тривалого часу не було чіткого визначення суті цього явища, що для права взагалі є критичним фактором. Адже брак чітко окресленого предмета регулювання стає неефективним або взагалі неможливим саме це регулювання.

Спроби сформулювати його були спрямовані насамперед на групування певних функціональних ознак мережі Інтернет. Наприклад, Інтернет визначали як універсальну систему об'єднаних мереж, які дають змогу забезпечити включення будь-яких масивів інформації для надання її користувачам, надання довідкових та інших інформаційних послуг, а також здійснення різних цивільно-правових угод на основі комбінації інформаційно-комунікаційних технологій²⁷⁵. Проте подібні йому формулювання не передбачали головного – можли-

²⁷⁵ Бачило І. Л. Информационное право. Основы практической информатики. – М., 2001. – с. 209 – 210.

вості чітко окреслити правовий статус цієї системи та суб'єктів, діяльність яких пов'язана з нею.

В українському законодавстві правове визначення поняття Інтернет міститься в нормах ст. 1 Закону України „Про телекомунікації”, згідно з яким *Інтернет це всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором та базується на Інтернет-протоколі, визначеному міжнародними стандартами.*²⁷⁶

На основі цього визначення можна сформулювати низку ключових ознак мережі Інтернет, що виражають особливості правового регулювання окремих її функцій.

По перше, Інтернет – це *інформаційна система*, тобто сукупність телекомунікаційних мереж і засобів для накопичення, оброблення, зберігання і передавання даних.

Інформаційна система Інтернет має ще дві додаткові ознаки, якими вона відрізняється від різних спеціалізованих, закритих, або локальних, інформаційних систем (наприклад, військових, банківських, локальних комп'ютерних систем і мереж різних установ, підприємств та організацій). Такими додатковими ознаками є *всесвітній характер доступу*, тобто відкритість Інтернет для доступу з будь-якої можливої точки Світу, де є необхідне обладнання, та *загальний характер доступу*, тобто можливість будь-якої особи без додаткових обмежень або дозволів отримати доступ та користуватися основними послугами Інтернет.

Невід'ємною характеристикою Інтернет є *глобальний адресний простір*, тобто сукупність адрес мережі Інтернет, за допомогою яких впорядковуються і зв'язуються між собою окремі інформаційні ресурси (Інтернет-сторінки) і користувач дістає можливість переходити від одного інформаційного ресурсу до іншого.

Згідно із Законом України „Про телекомунікації”, *адреса мережі Інтернет* – це визначений чинними в Інтернеті міжнародними стандартами цифровий та/або символічний ідентифікатор доменних імен в ієрархічній системі доменних назв. Фактично це назва, яка присвоюється окремому електронному інформаційному ресурсу – Інтернет-сторінці. Наприклад, адресою Інтернет-сторінки Верховної Ради України є <http://www.rada.gov.ua/>.

²⁷⁶ Про телекомунікації: Закон України // Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155.

Нарешті, останньою ключовою ознакою Інтернет є використання так званого *Інтернет-протокола*, який визначається міжнародними стандартами. Це й певний технічний стандарт, використання якого дає змогу окремим електронно-обчислювальним машинам з'єднуватися між собою, використовуючи дротові й бездротові телекомунікаційні мережі. Міжнародний характер цього технічного стандарту зумовлений глобальним характером Інтернет, за якого окремі держави не здатні вводити національні стандарти, що відрізняються від нього, оскільки це виключило б інформаційні мережі такої держави із загальної мережі.

Слід також виділити такий термін, як *національний сегмент мережі Інтернет*, який використовують у національних і міжнародних актах. Цей термін означає сукупність адрес Інтернет, яким присвоєно код країни, визначений міжнародними стандартами. Кожна держава має право визначати певні нормативно-правові стандарти і правила реєстрації, використання та адміністрування подібних адрес. *Український сегмент Інтернет* охоплює сукупність електронних інформаційних ресурсів, яким присвоєні адреси, побудовані на домені „UA”.

На основі зазначеного вище тлумачення сутності поняття „Інтернет” можна визначити основні підходи до правових аспектів цього явища:

Інтернет в цілому не є суб'єктом права. Це є сукупність інформаційного обладнання та інформаційних ресурсів. Але він не є ні міжнародною організацією, ні юридичною особою, ні будь-якою іншою організованою структурою, яка може вступати в правовідносини.

Інтернет у цілому не є об'єктом права. В Інтернет немає єдиного конкретного власника, як і немає такого суб'єкта, який би управляв або контролював досить значну частину цієї мережі. Понад те, через технічні особливості жодна складова Інтернет не є критичною для функціонування всієї системи.

Для правильного аналізу видів інформаційної діяльності, що проводиться за допомогою Інтернет, слід також визначити два основні способи розповсюдження інформації за допомогою цієї мережі: *активне* – через електронну пошту і *пасивне* – розміщення інформації на електронних сторінках, до яких споживач звертається самостійно. Ці види розповсюдження інформації мають принципово різні основи правового регулювання. Так, активне може здійснюватися проти волі її адресата. Масові розсилання рекламної або іншої інформації, яку

споживач не замовляв, дістали назву „спам”. Через це спочатку провайдерами Інтернет, а в деяких країнах і на законодавчому рівні застосовуються певні обмеження таких дій. Ключовим мотивом у цьому є те, що споживач змушений оплачувати прийняття електронних листів, які йому не потрібні.

Іншим важливим аспектом є те, що розміщення інформації на електронних сторінках є пасивним способом поширення інформації. Споживач самостійно, на власний розсуд, звертається до такої сторінки. Саме ця особливість поширення інформації в Інтернет дає змогу визначити, що *Інтернет в цілому не є засобом масової інформації*. Адже законодавство однозначно відносить Інтернет до одного із видів телекомунікацій, тобто до засобів передавання і приймання інформації в електронному вигляді. Власник інформаційного ресурсу не робить ніяких активних дій щодо доставки інформації до споживача. Натомість і друковані, і електронні ЗМІ (телебачення та радіомовлення) передбачають певні способи доставки інформації до споживача (розповсюдження через передплату, роздрібну торгівлю, трансляцію тощо).

Зазначимо, що спроби визначити Інтернет як якесь специфічне середовище, тобто як певну віртуальну субстанцію, може стати спробою вивести цей засіб комунікації з правового поля, що гарантує свободу слова, конфіденційність кореспонденції тощо. Подібні спроби вже робилися у деяких державах і були припинені лише завдяки ефективній роботі правозахисних механізмів. Так, у червні 1997 р. Верховний Суд США відкинув положення закону „*Про пристойність у засобах зв'язку*”, згідно з якими розповсюдження матеріалів непристойного змісту, до яких може отримати доступ неповнолітня особа, кваліфікується як злочин, оскільки це було б порушенням захищеного конституцією права свободи слова²⁷⁷.

В аспекті визначення правового статусу інформаційних ресурсів Інтернет та пов'язаних із цим питань захисту прав фізичних та юридичних осіб варто згадати також Постанову Вищого арбітражного суду України “Про питання захисту авторських прав в Інтернеті”, яка визнає, що розміщення творів у мережі Інтернет у вигляді, доступному для публічного споживання, є їх *відтворенням* у розумінні ст. 4 Закону України “Про авторське право і суміжні права”, у зв'язку з чим на розміщення творів в Інтернеті поширюється дія цього Закону.²⁷⁸

²⁷⁷ Див. : <http://www.aclu.org/>

²⁷⁸ Постанова Вищого Арбітражного суду України “Про питання захисту авторських прав в Інтернеті” від 5 червня 2000 р. № 04-1/5-7/82. // Вісн. господ. судочинства. – 2001. – № 2.

11. 2. Суб'єкти і об'єкти правовідносин у функціонуванні Інтернет.

Розглядаючи окремі види інформаційної діяльності, які проводяться в межах або за допомогою Інтернет, насамперед слід виділити їх неоднорідність. Тому правовідносини, що виникають з приводу функціонування Інтернет, не підлягають узагальненню. Навпаки, деякі дослідники акцентують увагу на необхідності запровадження певної класифікації як самих правовідносин щодо Інтернет, так і суб'єктів цих правовідносин. Так, пропонується виділяти щонайменше три групи суб'єктів, які діють в Інтернет²⁷⁹. Загалом сама ідея подібної диверсифікації є дуже слушною, але за основу все ж слід брати не стільки функціональну спрямованість діяльності того чи іншого суб'єкта, як правовий матеріал, яким відповідна діяльність регламентується.

Першу групу суб'єктів, що проводять інформаційну діяльність в Інтернет, становлять *оператори і провайдери телекомунікацій*. Вони забезпечують саме функціонування Інтернет як інформаційної системи. Їх діяльність охоплює: технічне обслуговування і експлуатацію технічного обладнання телекомунікаційних мереж, надання в користування ліній зв'язку, реєстрацію та адміністрування адрес Інтернет тощо.

Основними видами інформаційних послуг, які надаються цими суб'єктами, є:

- 1) *підключення*, тобто забезпечення доступом до Інтернет;
- 2) *хостинг* – розміщення інформації та інформаційних ресурсів замовника на відповідному технічному обладнанні – веб-серверах і забезпечення доступу до цих ресурсів через Інтернет;
- 3) *адміністрування* – здійснення організаційно-технічних заходів для забезпечення функціонування технічних засобів підтримки адресного простору Інтернет;
- 4) *послуги з навігації* в Інтернет – створення так званих веб-порталів, які полегшують пошук і доступ до інформаційних ресурсів Інтернет.

Діяльність цієї групи суб'єктів визначається насамперед національними та міжнародними нормативно-правовими актами, що регулюють питання електров'язку, телекомунікацій, надання інформаційних послуг тощо.

²⁷⁹ Див. напр.: *Копылов В. А.* Информационное право. – М. : Юристъ, 2002. – с. 238 – 239.

До другої групи суб'єктів належать *виробники, власники та розповсюджувачі інформації та інформаційних ресурсів*, тобто суб'єкти, які створюють інформаційне наповнення Інтернет. Ці суб'єкти створюють електронні інформаційні ресурси, володіють правами на них або на окремі документи, що входять до їх складу та забезпечують функціонування електронних інформаційних ресурсів і задоволення інформаційних потреб користувачів. Окремо слід виділити групу суб'єктів, яка надає специфічні послуги щодо укладання цивільно-правових угод за допомогою Інтернет (Інтернет-магазини, Інтернет-казино, Інтернет-аукціони, платні інформаційні послуги тощо), тобто все, що охоплюється терміном *e-commerce* (електронна комерція).

Діяльність суб'єктів цієї групи регулюється насамперед цивільним законодавством і законодавством про інтелектуальну власність та авторські права. Щодо електронної комерції, то незважаючи на нерегульованість цієї сфери в національному законодавстві слід зазначити, що Інтернет у цьому разі виступає лише *засобом комунікації* між продавцем і споживачем, подібним до телефонного або поштового зв'язку.

Ще однією особливістю застосування правового регулювання інформаційних ресурсів Інтернет є принцип застосування щодо них законодавства тієї країни, на території якої перебувають фізичні носії, на яких розміщені ці електронні інформаційні ресурси.

Останню, третю, групу становлять *споживачі телекомунікаційних послуг*. Споживачем може бути юридична або фізична особа, яка потребує, замовляє або отримує телекомунікаційні послуги для власних потреб. Основними видами послуг, які надаються користувачам Інтернет, є: підключення, доступ до інформаційних ресурсів, хостинг та електронна пошта.

При цьому основу правового регулювання становлять, по перше, конституційні норми, якими визначаються права і свободи людини в галузі інформації (свобода слова, таємниця кореспонденції), норми цивільного права та законодавства про захист прав споживачів. Окремо слід відзначити два типи цивільно-правових угод, які укладаються між операторами і провайдерами телекомунікацій та користувачами телекомунікаційних послуг та між власниками інформаційних ресурсів і користувачами цих ресурсів. Цими угодами можуть установлюватися додаткові правила використання послуг та обладнання, доступу до інформації та прав щодо користування нею.

Зазначена класифікація дає змогу окреслити основні об'єкти правовідносин в Інтернет. Це:

- телекомунікаційні мережі та інше технічне обладнання;
- комп'ютерне програмне забезпечення;
- інформація, інформаційні ресурси, інформаційні продукти та інформаційні послуги;
- доменні імена;
- права та свободи в галузі інформації;
- інформаційна безпека.

11. 3. Правові основи адміністрування домену UA.

Серед означених об'єктів правовідносин слід виділити такий специфічний, властивий лише Інтернет, як *доменні імена*.

Закон України „Про телекомунікації” (ст. 1) визначає, що *домен* – це частина ієрархічного адресного простору Інтернет, яка має унікальну назву, що її ідентифікує, обслуговується групою серверів доменних імен та централізовано адмініструється.

В українському сегменті Інтернет на законодавчому рівні виокремлюються:

- домен UA – це домен верхнього рівня ієрархічного адресного простору Інтернет, створений на основі кодування назв країн відповідно до міжнародних стандартів, для обслуговування адресного простору українського сегмента Інтернет;
- домен другого рівня – частина адресного простору мережі Інтернет, що розміщена на другому рівні ієрархії імен у цій мережі.

Ключовим аспектом забезпечення функціонування українського сегмента Інтернет є *адміністрування адресного простору*.

За ст. 56 Закону України „Про телекомунікації”, адміністрування адресного простору українського сегмента Інтернет включає комплекс організаційно-технічних заходів, необхідних для забезпечення функціонування технічних засобів підтримки адресування, у тому числі серверів доменних назв українського сегмента Інтернет, реєстру домену UA в координації з міжнародною системою адміністрування Інтернет, спрямованих на систематизацію та оптимізацію використання, обліку й адміністрування доменів другого рівня, а також створення умов для використання простору доменних імен на прин-

цях рівного доступу, захисту прав споживачів послуг Інтернет та вільної конкуренції.

Основними завданнями адміністрування адресного простору українського сегмента Інтернет, який здійснюється уповноваженою організацією, є:

- 1) створення реєстру доменних назв і адрес мережі українського сегмента Інтернет;
- 2) створення реєстру доменних назв у домені UA;
- 3) створення і підтримка автоматизованої системи реєстрації та обліку доменних назв і адрес українського сегмента Інтернет;
- 4) забезпечення унікальності, формування та підтримки простору доменних назв другого рівня в домені UA;
- 5) створення умов для використання адресного простору українського сегмента Інтернет на принципах рівного доступу, оптимального використання, захисту прав споживачів послуг Інтернет та вільної конкуренції;
- 6) представництва та захисту у відповідних міжнародних організаціях інтересів споживачів українського сегмента Інтернет.

Адміністрування у домені UA здійснюється недержавною організацією, яка утворюється організаціями операторів та провайдерів Інтернет зареєстрована відповідно до міжнародних вимог.

Утворення адресного простору, розподіл і надання адрес, маршрутизація інформації між адресами здійснюються відповідно до міжнародних вимог.

Згідно з розпорядження Кабінету Міністрів України “Про адміністрування домену UA передбачалося створення об’єднання підприємств „Український мережевий інформаційний центр” з метою управління адресним простором українського сегмента Інтернет, обслуговування та адміністрування системного реєстру і системи доменних імен домену верхнього рівня UA та подання листа про делегування відповідних функцій до Всесвітньої корпорації з призначення доменних імен та номерів (ICANN) ²⁸⁰.

Домен UA було зареєстровано приватною організацією ToЗВ “Коммуникационные системы” у грудні 1992 р. Нині адміністрування домену UA здійснюється ToЗВ “Хостмастер”. Ця організація формулює правила й визначає політику адміністрування для цього домену.

²⁸⁰ Про адміністрування домену UA: Розпорядження Кабінету Міністрів України від 22 липня 2003 р. N 447-р.

Законодавство й судова практика деяких країн приділяє значну увагу проблемі використання зареєстрованих назв фірм, товарних знаків, імен як адрес Інтернет-сайтів, оскільки використання відомих назв збільшує кількість відвідувань того чи іншого інформаційного ресурсу і її можна використовувати як засіб недобросовісної конкуренції.

11. 4. Декларація Ради Європи “Про свободу спілкування в Інтернет”.

Для того, щоб компроміс між інформаційними правами людини, з одного боку, і державним регулюванням та безпекою в Інтернет, у більшості розвинених держав пропонується йти шляхом розвитку саморегуляції і тісної співпраці з недержавним сектором, що надає мережеві послуги. Так, ще в 1997 р. *Європейський парламент схвалив резолюцію, на доповідь Комісії з протиправного та шкідливого змісту в Інтернет*²⁸¹.

Цією резолюцією було запропоновано класифікацію, за якою слід розрізняти матеріали протиправного і шкідливого змісту. *Матеріали протиправного змісту* – це інформація, що прямо порушує вимоги національних чи міжнародних правових актів. Водночас під інформацією зі шкідливим змістом розуміють інформацію, яка не є протиправною, але розповсюдження її обмежене (лише для дорослих, наприклад), а також інформація, яка може образити деяких користувачів, хоча її публікація не обмежена відповідно до принципу свободи самовираження. Стосовно цих двох категорій інформації потрібно застосовувати різні заходи.

За цією резолюцією, матеріалами протиправного змісту мають займатися за місцем їх створення правоохоронні органи, дії яких регулюються національним законодавством і угодами про судове співробітництво. Проте й сам Інтернет через системи саморегуляції, які добре функціонують, відповідно до існуючого законодавства і за підтримки споживачів, сприяє зменшенню обсягів розповсюдження матеріалів протиправного змісту (особливо дитячої порнографії і матеріалів расистського та антисемітського змісту).

Щодо матеріалів шкідливого змісту пропонується насамперед дати користувачам можливість самим вирішувати проблему виключ-

²⁸¹ European Parliament Resolution of 24 April 1997 on the Commission communication on illegal and harmful content on the Internet (COM (96) 483).

но технічними засобами (за допомогою систем фільтрації і рейтингової оцінки змісту), розширюючи обізнаність батьків і розвиваючи саморегулювання, яке здатне створити певні рамки, зокрема, щодо захисту неповнолітніх.

Така позиція стала ще актуальнішою після прийняття Радою Європи „Декларації про свободу спілкування в Інтернет”²⁸². Приймаючи цю Декларацію, Рада Європи виявила послідовність у дотриманні проголошених нею раніше принципів. Мета цієї Декларації – гарантування права на свободу інформації, встановленого ст. 10 Європейської Конвенції щодо захисту прав і основних свобод людини. Для цього в Декларації сформульовано сім основних принципів, які сприяють реалізації права на свободу слова в Інтернет.

Згідно з цими принципів держави-члени Ради Європи зобов’язуються:

- не встановлювати обмежень змісту інформації в Інтернет, більших, ніж ті, що існують щодо інших засобів доставки інформації;
- заохочувати саморегуляцію змісту інформації в Інтернет;
- зняти попередній державний контроль, зокрема, утриматися від використання блокувань і фільтрів, які перешкоджають доступу до інформації, крім фільтрів, що не допускають до інформації вразливі групи, наприклад, дітей до певних сайтів;
- утриматися від використання реєстраційних схем, які обмежують надання послуг через Інтернет;
- зняти перешкоди, які заважають забезпечити доступ до Інтернет або створення і функціонування Інтернет-сайтів для окремих верств суспільства;
- не зобов’язувати провайдерів проводити моніторинг усієї інформації, що проходить через їх сервер, та обмежити їх відповідальність за зміст інформації, котра передається з використанням їх послуг;
- гарантувати право на анонімність в Інтернет (крім випадків розслідування злочинів та розшуку злочинців).

²⁸² Declaration on freedom of communication on the Internet. Adopted by the Committee of Ministers at the 840th meeting of the Ministers’ Deputies. Strasbourg, 28. 05. 2003. / <http://www.coe.int/portal/T.asp>

11. 5. Національна програма інформатизації.

Значну роль у розвитку українського сегмента Інтернет відіграє *Національна програма інформатизації України*.

Згідно з положенням розділу III Концепції національної програми інформатизації, “державна політика інформатизації формується як складова частина соціально-економічної політики держави в цілому”²⁸³.

Нормами ст. 5 Закону “Про національну програму інформатизації”²⁸⁴ визначено, що головною метою цієї Програми є створення необхідних умов для забезпечення громадян та суспільства своєчасною, достовірною і повною інформацією шляхом широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави.

Програма спрямована на вирішення таких основних завдань:

- формування правових, організаційних, науково-технічних, економічних, фінансових, методичних та гуманітарних передумов розвитку інформатизації;
- застосування та розвиток сучасних інформаційних технологій у відповідних сферах суспільного життя України;
- формування системи національних інформаційних ресурсів; створення загальнодержавної мережі інформаційного забезпечення науки, освіти, культури, охорони здоров’я тощо;
- створення загальнодержавних систем інформаційно-аналітичної підтримки діяльності органів державної влади та органів місцевого самоврядування;
- підвищення ефективності вітчизняного виробництва на основі широкого використання інформаційних технологій;
- формування та підтримка ринку інформаційних продуктів і послуг;
- інтеграція України у світовий інформаційний простір.

Однак більшість дослідників, характеризуючи український сегмент Інтернет, звертають увагу на недостатні темпи розвитку його наповнення, причому це стосується як електронних інформаційних ресурсів, так і системи надання електронних інформаційних послуг та

²⁸³ Про Концепцію Національної програми інформатизації: Закон України від 4 лютого 1998 року № 75/98-ВР. // Відомості Верховної Ради України. – 1998. – № 27-28. – Ст. 182.

²⁸⁴ Про Національну програму інформатизації: Закон України від 4 лютого 1998 р. №74/98-ВР. // Відомості Верховної Ради України. – 1998. – № 27-28,. – Ст. 18.

електронної комерції. Так, український сегмент Інтернет є менший від російського і дуже відстає від польського, словацького, чеського, не кажучи вже про мережу розвинених країн. І це без урахування того, що за різними оцінками, від 90 до 95% ресурсів українського сегмента Інтернет є російськомовними.

Проте цю ситуацію варто розглядати, з позиції соціальних характеристик середньостатистичного користувача Інтернету. Так, у США й Канаді типовим користувачем Інтернету є особа, молодша 35 років, з високим рівнем прибутку, англomовний міський мешканець. У Росії (яка близька в цьому до України), доступ в Інтернет мають переважно мешканці міст-мільйонерів, студенти і працівники вищих навчальних закладів, НДІ та великих державних установ, промислових і фінансових організацій²⁸⁵. Таким чином, Інтернет можна вважати ефективним засобом “адресного” інформаційного впливу на людей, соціальний статус яких вищий за середні показники, і які становлять політично, економічно та соціально найбільш активну частину населення.

Першим національним нормативно-правовим актом, який стосувався безпосередньо питань Інтернет, був Указ Президента “Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні”²⁸⁶.

Цим указом визначається (п. 1), що розвиток національної складової глобальної інформаційної мережі, забезпечення широкого доступу до неї громадян і юридичних осіб усіх форм власності в Україні, належне представлення в ній національних інформаційних ресурсів є одним із пріоритетних напрямів державної політики у сфері інформатизації, задоволення конституційних прав громадян на інформацію, побудови відкритого демократичного суспільства, розвитку підприємництва.

Для досягнення таких цілей запропоновано такі заходи:

- створення у найкоротші строки належних економічних, правових, технічних та інших умов для забезпечення широкого доступу до Інтернет;

²⁸⁵ *Фельдман Д.* Информационная и национальная безопасность России (к годовщине принятия доктрины информационной безопасности Российской Федерации) // Власть. – 2001. - № 9. – С. 33.

²⁸⁶ Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні: Указ Президента України від 31 липня 2000 р. № 928/2000.

- розширення і вдосконалення подання в Інтернет об'єктивної інформації органів державної влади, місцевого самоврядування, установ, підприємств, організацій;
- забезпечення конституційних прав людини і громадянина на вільне збирання, зберігання, використання та поширення інформації, свободу думки і слова, вільне вираження своїх поглядів і переконань;
- забезпечення державної підтримки розвитку інфраструктури надання інформаційних послуг через Інтернет;
- розвиток та впровадження сучасних комп'ютерних інформаційних технологій;
- вирішення завдань щодо гарантування інформаційної безпеки держави, запобігання поширенню інформації, розповсюдження якої заборонено законодавством;
- удосконалення правового регулювання діяльності суб'єктів інформаційних відносин виробництва, використання, поширення та зберігання електронної інформаційної продукції, захисту прав на інтелектуальну власність, посилення відповідальності за порушення встановленого порядку доступу до електронних інформаційних ресурсів усіх форм власності, за навмисне поширення комп'ютерних вірусів.

Слід зазначити, що в цитованому Указі чітко й логічно вирішені питання інформаційної безпеки в Інтернет. Так, держава покладає на себе функції гарантування власної інформаційної безпеки та інформаційних прав і свобод людини. Забезпечення ж безпосередньо інформаційної безпеки людини, суспільства, різних юридичних осіб ґрунтується на створенні дієвих правових механізмів, за допомогою яких перелічені суб'єкти мали б можливість визначити і забезпечити необхідний, на їхню думку, рівень власної безпеки.

11. 6. Електронні документи та електронний документообіг.

Важливим кроком у розширенні використання електронних засобів зв'язку і, зокрема, Інтернет стало прийняття у травні 2003 р. Законів України “Про електронні документи та електронний документообіг”²⁸⁷ та “Про електронний цифровий підпис”²⁸⁸.

Закон України “Про електронні документи та електронний документообіг” дав єдине визначення електронного документа, визначив єдині вимоги до реквізитів електронного документа, надав йому юридичної сили.

Закон дає поняття електронного документообігу (ст. 9), як “сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів”.

Завданням державного регулювання у сфері електронного документообігу, відповідно до цього Закону (ст. 4), є:

- реалізація єдиної державної політики електронного документообігу;
- забезпечення прав і законних інтересів суб’єктів електронного документообігу;
- нормативно-правове забезпечення технології оброблення, створення, передавання, одержання, зберігання, використання та знищення електронних документів.

Одним із реквізитів електронного документа є електронний підпис. Згідно зі ст. 1 Закону України “Про електронний цифровий підпис”, *електронний цифровий підпис – це вид електронного підпису, отриманий за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача.*

Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

²⁸⁷ Про електронні документи та електронний документообіг: Закон України від 22 травня 2003 р. № 851-IV // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 275.

²⁸⁸ Про електронний цифровий підпис: Закон України від 22 травня 2003 р. № 852-IV // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 276.

Особистий ключ – це параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу.

Відкритий ключ – параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису.

Чинність і належність відкритого ключа підписувачу засвідчується за допомогою сертифікату відкритого ключа, який є документом, що розповсюджується в електронній формі або на папері та використовується для ідентифікації особи підписувача.

Законодавство виділяє два види сертифікатів ключів – прості й посилені. Останні мають право видавати лише акредитовані центри сертифікації ключів, засвідчувальні центри органів виконавчої влади та центральний засвідчувальний орган за умови повної відповідності параметрів криптографічного алгоритму формування та перевірки електронного цифрового підпису вимогам законодавства.

Електронний цифровий підпис, після необхідної перевірки за правовим статусом прирівнюється до власноручного підпису (печатки).

Функціонування системи електронного документообігу забезпечується комплексом спеціальних установ та організацій, до яких законодавство відносить:

Контролюючий орган (його функції виконує Адміністрація Державної служби спеціального зв'язку та захисту інформації України), що здійснює перевірку дотримання вимог законодавства центральним засвідчувальним органом, засвідчувальними центрами та центрами сертифікації ключів;

*Центральний засвідчувальний орган*²⁸⁹, який створюється Кабінетом Міністрів України та забезпечує в межах своїх повноважень створення умов для функціонування засвідчувальних центрів органів виконавчої влади або інших державних органів та центрів сертифікації ключів. Основними завданнями центрального засвідчувального органу є обслуговування посилених сертифікатів відкритих ключів центрів, а також їх акредитація.

*Засвідчувальні центри органів виконавчої влади, Центри сертифікації ключів, Акредитовані центри сертифікації ключів*²⁹⁰ надають по-

²⁸⁹ Про затвердження Положення про центральний засвідчувальний орган: Постанова Кабінету Міністрів України від 28 жовтня 2004 р. № 1451.

²⁹⁰ Про затвердження Порядку акредитації центру сертифікації ключів Постанова Кабінету Міністрів України від 13 липня 2004 р. № 903.

слуги, пов'язані з наданням особистих ключів для електронного цифрового підпису, їх сертифікатів, засвідчення їх чинності.

Особливі правила застосування електронного цифрового підпису встановлено для органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій державної форми власності²⁹¹. Так зазначеним вище установам дозволяється застосовувати електронний цифровий підпис лише за умови використання надійних засобів електронного цифрового підпису.

Така надійність засобів електронного цифрового підпису має бути підтверджена сертифікатом відповідності або позитивним висновком за результатами державної експертизи у сфері криптографічного захисту інформації, отриманим на ці засоби від адміністрації Держспецзв'язку.

Застосування електронного цифрового підпису для вчинення правочинів за участю інших юридичних та фізичних осіб можливе лише за наявності у них посиленних сертифікатів відкритих ключів.

Застосування електронного цифрового підпису забороняється:

- для складання електронних документів, які не можуть бути оригіналами у випадках, передбачених законодавством;
- для вчинення правочинів на суму, що перевищує 1 млн. гривень.

Сучасна система електронного документообігу в Україні лише починає формуватися, але вже існує досвід її застосування, в тому числі і у сфері діяльності органів виконавчої влади.

11. 7. Концепція створення “електронного уряду”.

Іншим напрямом діяльності держави в Інтернет є створення засад так званого електронного уряду – *e-government*, тенденції, яка швидко розвивається в багатьох розвинених країнах світу. Якщо головна її мета – забезпечення за допомогою Інтернет прямого інтерактивного контакту між громадянами та урядовими установами є поки що перспективою, то перший її етап – інформативний вже набув практичного втілення. В Україні вже діють електронні сторінки більшості органів державної влади та низки органів місцевого самоврядування. Було

²⁹¹ Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності: Постанова Кабінету Міністрів України від 28 жовтня 2004 р. № 1452.

також створено і правову базу, яка регулює порядок розміщення таких сторінок в Інтернеті та їх наповнення.

Піонером у цьому напрямі виявилася законодавча влада. Так, Розпорядженням Голови Верховної Ради було затверджено положення про веб-сайт Верховної Ради. Згідно з цим нормативно-правовим актом, веб-сайт Верховної Ради України є офіційним джерелом інформації ВР, який утворюється для висвітлення діяльності ВР, її органів та апарату, взаємного обміну інформацією з органами державної влади України та органами місцевого самоврядування з питань, пов'язаних з діяльністю Верховної Ради України, інформаційної взаємодії з урядовими і неурядовими організаціями країн світового співтовариства, громадськістю.²⁹²

Відразу зазначимо, що вперше в Україні електронний документ було названо офіційним джерелом інформації. Щоправда стосовно нормативно-правових актів який спосіб офіційної публікації не передбачений ні Регламентом Верховної Ради²⁹³, ані відповідним Указом Президента²⁹⁴.

Щодо веб-сайту Верховної Ради, то згідно з нормами вищезазначеного Положення, забороняється використовувати веб-сайт Верховної Ради України для цілей, не пов'язаних із діяльністю Верховної Ради України та її органів, з метою отримання прибутку, а також з порушенням законодавства України. Визначено також основні рубрики інформаційного наповнення сайту, які охоплюють бази законодавства та законопроектів, інформацію про діяльність Верховної Ради, депутатський корпус, структуру й апарат Верховної Ради, посилання на сайти парламентів інших країн. Передбачена можливість розміщення за принципом рівності веб-сторінок депутатських груп і фракцій, структурних підрозділів Верховної Ради.

Передбачено (п. 9 Розпорядження), що за розпорядженням Голови Верховної Ради доступ до відповідної веб-сторінки на веб-сайті Верховної Ради України може бути обмежений:

- за поданням Комітету Верховної Ради України з питань Регламенту, депутатської етики та організації роботи Верховної Ради України – до веб-сторінки депутатської фракції (групи), комітету і тимчасової комісії Верховної Ради України;

²⁹² Про положення про веб-сайт Верховної Ради України у глобальній інформаційній мережі Інтернет: Розпорядження Голови Верховної Ради України від 24 травня 2001 р. № 462.

²⁹³ Регламент Верховної Ради України від 27 липня 1994 р. № 129/94-ВР // Відомості Верховної Ради. – 1994. – № 35. – Ст. 338.

²⁹⁴ Про порядок офіційного оприлюднення нормативно-правових актів та набрання ними чинності: Указ Президента України від 10 червня 1997 р. № 503/97.

- за поданням керівника апарату Верховної Ради України – до веб-сторінки структурного підрозділу апарату Верховної Ради України.

Інформаційне забезпечення Верховної Ради України є одним з найбільш розвинених серед органів державної влади. Наприклад, Розпорядженням Голови Верховної Ради „Про Перелік автоматизованих систем інформаційно-технологічного забезпечення діяльності Верховної Ради України”²⁹⁵ визначається комплекс із 12 таких автоматизованих систем, які об’єднують 36 окремих баз даних. Перелік автоматизованих систем Верховної Ради включає:

- “Контроль проходження законопроектів”
- “Проходження законопроектів у структурних підрозділах апарату”
- комп’ютерну технологію інтегрованої обробки текстів законопроектів для підготовки до розгляду Верховною Радою України „ЗАКОНОТВОРЕЦЬ”
- “Автоматизовану систему документообігу
- “Листи та звернення громадян”
- “Автоматизовану систему запитів народних депутатів України, доручень Верховної Ради України”
- “Кадри”
- Інформаційно-пошукову систему “ЗАКОНОДАВСТВО”
- Систему “РАДА”
- Систему “Графіт”
- Інформаційно-пошукову систему “Адміністративно-територіальний устрій України”
- Програмний комплекс “Відрядження”

Правову основу розміщення в Інтернет інформації органів виконавчої влади було створено з прийняттям на початку 2002 р. Постанови Кабінету Міністрів “Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади”²⁹⁶. Головною метою оприлюднення інформації органів виконавчої влади в Інтернет (п. 1) є підвищення ефективності та прозорості діяльності цих органів шляхом впровадження та використання сучасних інформаційних технологій для надання інформаційних та інших послуг громадськості, забезпечення її впливу на процеси, що відбуваються у державі.

²⁹⁵ Про Перелік автоматизованих систем інформаційно-технологічного забезпечення діяльності Верховної Ради України: Розпорядження Голови Верховної Ради України від 1 липня 2003 року № 663.

²⁹⁶ Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади: Постанова Кабінету Міністрів України від 4 січня 2002 р. № 3.

Шляхами оприлюднення відповідної інформації є:

- розміщення і періодичне оновлення міністерствами, іншими центральними та місцевими органами виконавчої влади інформації відповідно до вимог цього Порядку на власних веб-сайтах;
- створення Єдиного веб-порталу Кабінету Міністрів України, призначеного для інтеграції веб-сайтів органів виконавчої влади та розміщення інформаційних ресурсів відповідно до потреб громадян.

Було визначено також норми визначення порядку захисту інформації, розміщеної в Інтернет. Зокрема, передбачено, що інформація, яка розміщується на веб-сайтах органів виконавчої влади та Веб-порталі, повинна мати захист від несанкціонованої модифікації. Інформаційне наповнення, захист інформації від несанкціонованої модифікації й технічне забезпечення функціонування веб-сайтів міністерств, інших центральних та місцевих органів виконавчої влади як складових частин веб-порталу зазначені органи здійснюють самостійно. Контроль за дотриманням вимог захисту інформації, доступної через веб-портал, здійснюється Департаментом спеціальних телекомунікаційних систем та захисту інформації СБУ.

Законодавством також визначено особливий порядок використання органами виконавчої влади послуг Інтернет, який визначається Постановою Кабінету Міністрів України „Про затвердження Порядку підключення до глобальних мереж передачі даних”²⁹⁷. Зокрема, цією постановою встановлено правовий статус домену gov.ua як офіційної Інтернет-адреси органів державної виконавчої влади.

Органи виконавчої влади та інші державні органи зобов’язані реєструвати свою адресу виключно на домені gov. ua.

Інші державні підприємства, установи та організації, які одержують, обробляють, поширюють і зберігають інформацію, що є об’єктом державної власності та охороняється згідно із законодавством, реєструють свої адреси в домені ua.

Вказані абоненти підключаються до глобальних мереж лише через операторів. Абонент зобов’язаний укласти з оператором договір про надання послуг з доступу до глобальних мереж та протягом п’ятнадцяти робочих днів повідомити про це Міністерство транспорту і зв’язку.

Локальні обчислювальні мережі, а також окремі електронні обчислювальні машини, на яких обробляють або зберігають інформа-

²⁹⁷ Про затвердження Порядку підключення до глобальних мереж передачі даних: Постанова Кабінету Міністрів України від 12 квітня 2002 р. № 522.

цію з обмеженим доступом, що є об'єктом державної власності і охороняється згідно із законодавством, забороняється підключати до глобальних мереж.

Наступні кроки на шляху правового забезпечення інформаційної діяльності органів в Інтернет було визначено Постановою Кабінету Міністрів України „Про заходи щодо створення електронної інформаційної системи „Електронний Уряд””²⁹⁸.

Цією Постановою, зокрема, визначено, що одним з пріоритетних завдань розвитку інформаційного суспільства є надання громадянам і юридичним особам інформаційних та інших послуг шляхом використання електронної інформаційної системи „Електронний Уряд”, яка забезпечує інформаційну взаємодію органів виконавчої влади між собою, з громадянами та юридичними особами на основі сучасних інформаційних технологій.

Центральною частиною “Електронного Уряду” є *Єдиний веб-портал органів виконавчої влади*, який призначено для інтеграції веб-сайтів, електронних інформаційних систем і ресурсів надання інформаційних та інших послуг з використанням Інтернет. Цей веб-портал розміщено за адресою <http://www.kmu.gov.ua/>.

11. 8. Національний реєстр електронних інформаційних ресурсів.

Прискорення розвитку українського сегмента Інтернет було покладено в основу Концепції формування системи національних електронних інформаційних ресурсів, затвердженої розпорядженням Кабінету Міністрів України²⁹⁹. За цією Концепцією, національними електронними інформаційними ресурсами (національні ресурси) є ресурси незалежно від їх змісту, форми, часу та місця створення, форми власності, призначені для задоволення потреб громадянина, суспільства, держави. За формою власності національні ресурси поділяються на державні, комунальні та приватні.

З метою запровадження єдиної системи обліку електронних інформаційних ресурсів держави в Україні створено Національний реєстр електронних інформаційних ресурсів (Національний реєстр).

²⁹⁸ Про заходи щодо створення електронної інформаційної системи “Електронний Уряд” Постановою Кабінету Міністрів України від 24 лютого 2003 р. № 208.

²⁹⁹ Про затвердження Концепції формування системи національних електронних інформаційних ресурсів: Розпорядження Кабінету Міністрів України від 5 травня 2003 р. № 259-р.

Національний реєстр – це інформаційно-телекомунікаційна система, призначена для реєстрації, обліку, накопичення, оброблення і зберігання відомостей про склад, зміст, розміщення, умови доступу до електронних інформаційних ресурсів та задоволення потреб юридичних і фізичних осіб в інформаційних послугах³⁰⁰.

Замовником і утримувачем Національного реєстру є Міністерство транспорту та зв'язку України, а його адміністратором – уповноважена Мінтрансзв'язку юридична особа. Сам Національний реєстр складається з еталонного, робочого, страхового та інформаційного фондів, до яких обов'язково включаються е-ресурси органів державної влади, органів місцевого самоврядування та інших юридичних осіб публічного права, доступ до яких здійснюється через телекомунікаційні мережі загального користування.

Власник е-ресурсу зобов'язаний зареєструвати ресурс протягом 30 днів після надання користувачам доступу до нього і несе відповідальність за достовірність поданих у заяві відомостей згідно із законодавством.

Включення до Національного реєстру е-ресурсів приватної форми власності здійснюється на добровільних засадах.

Певні суперечки викликав прийнятий Міністерством транспорту та зв'язку „Порядок проведення державної реєстрації електронних інформаційних ресурсів”³⁰¹, правила якого поширюються як на державні так і на приватні е-ресурси. Насамперед через те, що, як вже зазначалося вище, світова практика намагається оминати додаткові реєстраційні схеми та запровадження цензури в Інтернет.

Натомість п. 3. 3 зазначеного Порядку визначає вимоги, недодержання яких є підставою для відмови в реєстрації або припинення реєстрації е-ресурсу в Національному реєстрі. Так, до Національного реєстру не включаються е-ресурси, які містять:

- відомості, що становлять державну таємницю;
- інформацію з обмеженим доступом;
- інформацію, розповсюдження якої заборонене законодавством.

Е-ресурс не повинен містити:

- закликів до захоплення державної влади, насильницької зміни конституційного ладу, порушення територіальної цілісності і недоторканності України;

³⁰⁰ Про затвердження Положення про Національний реєстр електронних інформаційних ресурсів: Постанова Кабінету Міністрів України від 17 березня 2004 р. № 326.

³⁰¹ Про затвердження Порядку проведення державної реєстрації електронних інформаційних ресурсів: Наказ Міністерства транспорту та зв'язку України від 27 березня 2005 № 153.

- інформації, що містить пропаганду тероризму, війни, геноциду або культу насильства і жорстокості;
- інформації, що дискримінує особу за ознаками раси, кольору шкіри, політичних, релігійних та інших переконань, статі, етнічного чи соціального походження, майнового стану, місця проживання, за мовними або іншими ознаками;
- інформації, що може зашкодити честі, гідності або діловій репутації окремих осіб;
- інформації, яка містить ненормативну лексику;
- інформації порнографічного характеру.

Державну реєстрацію е-ресурсів здійснює Державний департамент з питань зв'язку та інформатизації для чого у його складі створено спеціальну Комісію з ухвалення рішень про державну реєстрацію електронних інформаційних ресурсів. У разі прийняття Комісією рішення про державну реєстрацію е-ресурсу, а також за умови внесення власником е-ресурсу установленної оплати, власнику видається Свідоцтво про реєстрацію електронного інформаційного ресурсу встановленого зразка. Це свідоцтво є підставою для включення е-ресурсу до Національного реєстру.

Дати однозначну оцінку такого підходу до формування системи національних електронних ресурсів досить важко. З одного боку, ведення Національного реєстру сприятиме впорядкуванню системи е-ресурсів та спрощенню доступу до неї, з другого – за оцінками багатьох фахівців, запровадження додаткових реєстраційних схем може призвести до того, що частина е-ресурсів просто буде переміщена за кордон, за межі дії українського законодавства. Відповідно прибутки від надання послуг по хостингу та адміністрування будуть отримувати іноземні провайдери.

Загалом же, характеризуючи стан правового регулювання функціонування Інтернет, слід зазначити, що останніми роками було створено досить значну нормативно-правову базу. Але, на жаль, вона несе в собі традиційні для нашої правової системи спроби запровадження надмірного державного контролю і не завжди сприймає відповідні міжнародно-правові стандарти і досвід. Разом із тим, ще потребують врегулювання питання електронної комерції, надання інформаційних послуг, укладання цивільно-правових угод за допомогою Інтернет, забезпечення таємниці кореспонденції та інформаційної безпеки тощо.

ГЛАВА 12

ПРАВОВЕ РЕГУЛЮВАННЯ РОЗПОВСЮДЖЕННЯ МАСОВОЇ ІНФОРМАЦІЇ

Політико-правовий контекст діяльності у сфері масової інформації. Друковані засоби масової інформації (преса). Видавнича справа. Інформаційні агентства. Електронні засоби масової інформації. Розповсюдження і демонстрування фільмів.

12. 1. Політико-правовий контекст діяльності у сфері масової інформації

Одним із найбільш важливих для окремої людини, суспільства та держави видів інформації є масова інформація. За ст. 20 Закону України “Про інформацію”, масова інформація визначається як публічно поширювана друкована та аудіовізуальна інформація. Головним критерієм розмежування цього виду інформації й інших видів *критерій публічної поширюваності*, який означає масове розповсюдження цієї інформації для відносно великого, невизначеного кола осіб. Адже споживачем масової інформації як інформаційного продукту може стати будь-яка зацікавлена особа.

Законодавство визначає також засоби поширення масової інформації, які класифікуються залежно від форми подання інформації друкованої чи аудіовізуальної на:

- друковані засоби масової інформації – періодичні друковані видання (газети, журнали, бюлетені тощо) і разові видання з визначеним тиражем.
- аудіовізуальні засоби масової інформації – радіомовлення, телебачення, кіно, звукозапис, відеозапис тощо.

Як уже зазначалося вище, ключовою для розуміння сутності правового регулювання мас-медіа є їх дуалістична природа, яка полягає в тому, що, з одного боку, вони є звичайними підприємствами, а з другого – трибуною для висловлювання поглядів і демократичної комунікації³⁰². У цьому аспекті правові питання діяльності за-

³⁰² Крос К., Гакет Р. Політична комунікація і висвітлення новин у демократичних суспільствах: перспективи конкуренції. – К. : Основи, 2000. – с. 18.

собів масової інформації є невід’ємною частиною питань організації політичної влади в державі і залежать від ступеня демократичності цієї влади.

Найбільш популярною для визначення ролі і місця засобів масової інформації в сучасному демократичному суспільстві є так звана концепція “ліберального плюралізму”. Відповідно до цієї концепції, засоби масової інформації виконують три основні ролі: громадсько-го спостерігача, представника споживача та джерела суспільної інформації³⁰³.

Виконуючи роль *громадського спостерігача*, засоби масової інформації мають забезпечувати контроль за публічною владою, прозорість діяльності органів публічної влади, інформуючи громадськість про можливі зловживання та правопорушення в цій сфері, акцентуючи увагу владних інституцій на питаннях що викликають суспільний інтерес. Роль громадського спостерігача історично закріпилася за мас-медіа як одним із засобів захисту прав людини від можливих утисків з боку держави.

Роль засобів масової інформації як *представника споживача* полягає в тому, що, маючи на меті задоволення інформаційних потреб споживачів інформації, мас-медіа повинні йти назустріч цим потребам. Таким чином, певною мірою зміст інформації, яку поширюють мас-медіа, формується в рамках ринкового механізму, відповідно до попиту і пропозиції. Відповідно через ринкові механізми громадськість, суспільство в цілому та окремі соціальні групи можуть забезпечити представництво своїх інтересів у сфері масової інформації, через ЗМІ, що розраховані на відповідну аудиторію.

Нарешті, в ролі *джерела суспільної інформації* ЗМІ забезпечують притаманний демократичному суспільству процес вільного висловлювання ідей і поглядів кожним бажаним та широкого суспільного обговорення важливих проблем державного й суспільного життя. Така роль ЗМІ сприяє формуванню громадської думки та участі громадськості в політичному та суспільному житті держави.

Слід зазначити, що визначена вище концепція може бути реалізована лише за однієї умови – за незалежності ЗМІ. Саме на забезпечення такої незалежності спрямовані більшість правових гарантій діяльності ЗМІ.

³⁰³ Там само. – С. 45–46.

Зокрема, слід зазначити, що ч. 2 ст. 15 Конституції України в нашій державі цензура заборонена. Така пряма заборона фактично є ключовою гарантією свободи діяльності у сфері масової інформації. Хоча питання незалежності ЗМІ певною мірою є фікцією, адже всі вони мають своїх власників, які багато в чому визначають напрями діяльності кожного конкретного ЗМІ. Подібний стан речей характеризується терміном “економічна цензура”. В цьому разі слід говорити швидше про норми вже згаданої ст. 15 Конституції України, за якими суспільне життя в Україні ґрунтується на політичній, економічній та ідеологічній багатоманітності, а жодна ідеологія не може бути визнана державою як обов’язкова. Саме різноманітність, тобто належність ЗМІ від різних власників і, відповідно, розповсюдження за їх допомогою різних думок, поглядів та оцінок дає змогу створити загальний ефект незалежності ЗМІ.

Наприклад, можна виділити чотири основні види ЗМІ, залежно від статусу їх власників і засновників:

1) державні (офіційні), засновниками яких є органи публічної влади і які використовуються насамперед для розповсюдження інформації цих органів влади та діють у рамках державної інформаційної політики;

2) партійні, засновниками яких є політичні партії і які мають відповідне ідеологічне спрямування та використовуються насамперед для проведення політичної агітації;

3) приватні (незалежні), засновниками та власниками яких є суб’єкти господарської діяльності та які орієнтовані насамперед на отримання прибутку від здійснення інформаційної діяльності. Відповідно зміст діяльності цих ЗМІ визначається вимогами ринку інформаційних продуктів та послуг;

4) громадянські (неприбуткові), засновниками яких виступають і громадські організації (правозахисні, національні, культурні, релігійні, екологічні, професіональні тощо). Цей вид ЗМІ розрахований передусім на задоволення інформаційних потреб відповідних соціальних груп або інформування суспільства з питань діяльності відповідних громадських організацій.

12. 2. Друковані засоби масової інформації (преса)

Одним із найбільш давніх засобів поширення масової інформації є друковані ЗМІ – преса.

За ст. 1 Закону України “Про друковані засоби масової інформації (пресу) в Україні”³⁰⁴, під *друкованими засобами масової інформації (пресою)* в Україні розуміються періодичні і такі, що продовжуються, видання, які виходять під постійною назвою, з періодичністю один і більше номерів (випусків) протягом року на підставі свідоцтва про державну реєстрацію.

Таким чином, основними характеристиками друкованих ЗМІ є:

- періодичність видання (щонайменше один раз на рік);
- постійна назва, що об’єднує всі випуски;
- державна реєстрація як друкованого ЗМІ.

Відповідно під *діяльністю друкованих засобів масової інформації*, цей Закон (ст. 6) визначає такі дії, як: *збирання, творення, редагування, підготовка інформації до друку та видання друкованих засобів масової інформації з метою її поширення серед читачів.*

При цьому *продукцією друкованого ЗМІ є виготовлений видавцем тираж окремого випуску видання, підписаний редактором (головним редактором) на вихід у світ.*

Законодавство визначає перелік суб’єктів діяльності друкованих ЗМІ, кожен з яких має свій правовий статус і відповідно є носієм комплексу специфічних прав та обов’язків. До основних суб’єктів діяльності друкованих ЗМІ, зокрема, належать:

- *засновник (співзасновники)* – особа, яка заснувала засіб масової інформації, або особи, які об’єдналися з метою спільного заснування видання;
- *редактор (головний редактор)* – керівник редакції, уповноважений на те засновником;
- *редакція* – установа, що здійснює підготовку та випуск у світ друкованого засобу масової інформації за дорученням засновника;
- *журналіст* – творчий працівник, який професійно збирає, одержує, створює і займається підготовкою інформації для друкованого засобу масової інформації та діє на підставі трудових

³⁰⁴ Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16 листопада 1992 р. № 2782-XII // Відомості Верховної Ради України. – 1993. – № 1. – Ст. 1.

чи інших договірних відносин з його редакцією або займається такою діяльністю за її уповноваженням;

- *видавець* – суб'єкт підприємницької діяльності, який здійснює функції матеріально-технічного забезпечення видання друкованого засобу масової інформації на підставі пред'явлення засновником (співзасновниками) свідоцтва про його державну реєстрацію і укладеного між ними договору;
- *розповсюджувач* – суб'єкт підприємницької діяльності, який продає, надсилає за передплатою чи іншим способом розповсюджує виданий тираж періодичного і такого, що продовжується, видання, є розповсюджувачем продукції друкованого засобу масової інформації.

Виробничі, майнові та фінансові відносини засновника (співзасновників), редакції, видавця, розповсюджувача друкованого засобу масової інформації будуються на основі чинного законодавства і договору.

Слід зазначити, що деякі суб'єкти діяльності друкованих ЗМІ можуть одночасно по'єднувати в одній особі функції декількох інших суб'єктів. Так, *засновник* або *співзасновники* друкованого ЗМІ може по'єднувати в одній особі редакцію, видавця, розповсюджувача. А *редакція* друкованого ЗМІ має право виступати засновником або співзасновником, видавцем, розповсюджувачем.

Однією з особливостей створення друкованих ЗМІ є достатньо широкий, порівняно з іншими видами ЗМІ, перелік осіб, які мають право виступати як засновники. Так, право на заснування друкованого засобу масової інформації можуть мати:

- громадяни України, громадяни інших держав та особи без громадянства, не обмежені в цивільній правоздатності та цивільній дієздатності;
- юридичні особи України та інших держав;
- трудові колективи підприємств, установ і організацій на підставі відповідного рішення загальних зборів (конференції).

Юридичні особи можуть виступати як засновники друкованих ЗМІ навіть у випадках, коли цей вид діяльності не передбачений їхніми статутами.

Законодавством встановлено гарантії від монополізації друкованих засобів масової інформації, які реалізуються встановленням обмежень щодо засновників загальнодержавних і регіональних

громадсько-політичних ЗМІ. Фізична або юридична особа не може бути засновником або співзасновником чи контролювати більше як 5 відсотків таких видань.

У вітчизняному законодавстві можна виділити кілька основ класифікації друкованих ЗМІ, які зумовлюють особливості державної реєстрації та застосування до них деяких регуляторних актів щодо оподаткування та державної підтримки. До таких основ класифікації, зокрема, належать: сфера розповсюдження, вид видання, статус видання, програмні цілі або тематична спрямованість, категорія читачів, цільове призначення.

За *сферою розповсюдження* розрізняють друковані ЗМІ: зарубіжні (більше однієї країни), загальнодержавні, регіональні (дві і більше областей), місцеві.

За *видом видання* можна назвати такі друковані ЗМІ, як: газета, журнал, збірник, бюлетень, альманах, календар, дайджест тощо.

За *статусом* видання можуть бути вітчизняні (засновник або всі співзасновники є фізичними або юридичними особами-резидентами), спільні (хоча б один із співзасновників є іноземною фізичною або юридичною особою).

Відповідно до *категорії читачів* визначають ті верстви населення, на які розраховане видання: усе населення, дорослі, молодь, діти, чоловіки, жінки, інваліди, студенти, працівники певної галузі, науковці, педагоги тощо

Програмні цілі (або тематична спрямованість видання) характеризують завдання, які ставить перед собою засновник друкованого ЗМІ.

Нарешті, важливою характеристикою є *вид видання за цільовим призначенням*: загальнополітичне, з питань економіки і бізнесу, виробничо-практичне, наукове, науково-виробниче, науково-популярне, навчальне, довідкове, літературно-художнє, з питань мистецтва, спортивне, юридичне, для дозвілля, медичне, релігійне, уфологічне, екологічне, туристичне, , інформаційне, для дітей тощо. Окремо слід виділити такі види видань, як рекламне (понад 40% обсягу одного номера – реклама) та еротичне оскільки на дані види видань не розповсюджуються встановлені законодавством пільги, а з останніх стягується більший порівняно з іншими реєстраційний збір.

Друкований засіб масової інформації може бути виданий після його державної реєстрації. Порядок державної реєстрації визначаєть-

ся Законом “Про друковані засоби масової інформації (пресу) в Україні” та Положенням про державну реєстрацію друкованих засобів масової інформації в Україні³⁰⁵.

Зокрема, здійснюється реєстрація друкованих ЗМІ:

- загальнодержавної, регіональної та зарубіжної сфери розповсюдження – Міністерством юстиції;
- місцевої сфери розповсюдження – Головним управлінням юстиції Міністерства юстиції України в Автономній Республіці Крим, головними управліннями юстиції в областях, містах Києві та Севастополі.

У заяві про державну реєстрацію друкованого засобу масової інформації мають бути зазначені:

- 1) засновник (співзасновники) видання;
- 2) вид видання;
- 3) назва видання;
- 4) мова видання;
- 5) сфера розповсюдження (місцева, регіональна, загальнодержавна, зарубіжна) та категорії читачів;
- 6) програмні цілі (основні принципи) або тематична спрямованість;
- 7) передбачувані періодичність випуску, обсяг і формат видання;
- 8) юридична адреса засновника, кожного із співзасновників та його (їх) банківські реквізити;
- 9) місцезнаходження редакції.

Реєструючий орган має право зажадати від засновника (співзасновників) подання документів, якими підтверджується його (їх) цивільна правоздатність та цивільна дієздатність (паспорт, статут, договір між співзасновниками, договір з правонаступником, довіреність тощо).

Заява про реєстрацію друкованого ЗМІ розглядається у місячний строк з дня її одержання реєструючим органом, який за результатами розгляду заяви приймає одне з таких рішень:

- про державну реєстрацію;
- про відмову в державній реєстрації;
- про зупинення строку розгляду заяви про державну реєстрацію;
- про визнання недійсним свідоцтва про державну реєстрацію друкованого ЗМІ (на підставі письмового повідомлення за-

³⁰⁵ Про затвердження Положення про державну реєстрацію друкованих засобів масової інформації в Україні та Положення про державну реєстрацію інформаційних агентств як суб’єктів інформаційної діяльності: Наказ Міністерства юстиції України від 21 лютого 2006 р. № 12/5.

сновника (співзасновників), погодженого з редакцією, або рішення суду про припинення випуску друкованого засобу масової інформації).

За державну реєстрацію друкованих ЗМІ сплачується збір у розмірах, установлених Кабінетом Міністрів України³⁰⁶.

Після оформлення реєструвальним органом рішення про державну реєстрацію та сплати збору за державну реєстрацію зареєстрованому друкованому ЗМІ присвоюються відповідний номер і серія, а заявникові видається свідоцтво встановленого зразка. Після державної реєстрації друкованого ЗМІ його редакція набуває статусу юридичної особи.

Законодавство встановлює також певні вимоги до продукції друкованих засобів масової інформації, які стосуються *вихідних даних* та *контрольних примірників* видання.

За ст. 32 Закону “Про друковані засоби масової інформації (пресу) в Україні”, у кожному випуску друкованого засобу масової інформації мають бути *вихідні дані*: 1) назва видання; 2) засновник (співзасновники); 3) прізвище та ініціали редактора (головного редактора); 4) порядковий номер випуску і дата його виходу в світ; 5) індекс видання, розповсюджуваного за передплатою; 6) тираж; 7) ціна або помітка “Безкоштовно”; 8) адреси редакції, видавця, друкарні; 9) серія, номер і дата видачі свідоцтва про державну реєстрацію; 10) видавець (співвидавці).

Законодавством забороняється розповсюдження продукції друкованого засобу масової інформації без вихідних даних.

Ст. 33 цього Закону вимагає від редакції обов’язково безкоштовно надсилати засновникові (співзасновникам) і реєструючому органу контрольні примірники періодичних і таких, що продовжуються, видань відразу після надрукування.

12. 3. Видавнича справа

З інформаційною діяльністю в галузі друкованої масової інформації тісно пов’язана діяльність у сфері видавничої справи. Ст. 2 Закону України “Про видавничу справу”³⁰⁷ визначає *видавничу справу як сферу суспільних відносин, що поєднує в собі організаційно-творчу*

³⁰⁶ Про державну реєстрацію друкованих засобів масової інформації, інформаційних агентств та розміри реєстраційних зборів: Постанова Кабінету Міністрів України від 17 листопада 1997 р. № 1287.

³⁰⁷ Закон України “Про видавничу справу” від 5 червня 1997 р. № 318/97-ВР // Відомості Верховної Ради України. – 1997. – № 32. – Ст. 206.

та виробничо-господарську діяльність юридичних і фізичних осіб, зайнятих створенням, виготовленням і розповсюдженням видавничої продукції.

Складовими частинами видавничої справи є:

- *видавнича діяльність* – сукупність організаційних, творчих, виробничих заходів, спрямованих на підготовку і випуск у світ видавничої продукції;
- *виготовлення видавничої продукції* – виробничо-технологічний процес відтворення визначеним тиражем видавничого оригіналу поліграфічними чи іншими технічними засобами;
- *розповсюдження видавничої продукції* – доведення видавничої продукції до споживача як через торговельну мережу, так і іншими способами.

Відповідно до визначених складових видавничої справи, цей (ст. 10) виділяє три основних суб'єкти інформаційної діяльності в цій сфері, до яких належать:

- *видавець* – фізична чи юридична особа, яка здійснює підготовку і випуск видання;
- *виготовлювач видавничої продукції* – фізична чи юридична особа, що здійснює виготовлення замовленого тиражу видання;
- *розповсюджувач видавничої продукції* – фізична чи юридична особа, яка займається розповсюдженням видавничої продукції.

З метою обліку суб'єктів видавничої справи ведеться Державний реєстр України видавців, виготовників і розповсюджувачів видавничої продукції. Порядок внесення суб'єктів видавничої справи до відповідного Державного реєстру визначена Кабінетом Міністрів України згідно з Постановою “Про Державний реєстр видавців, виготівників і розповсюджувачів видавничої продукції”³⁰⁸.

Внесення суб'єктів видавничої справи до Державного реєстру здійснюється Державним комітетом з телебачення і раіомовлення України (Держкомтелерадіо) та його місцевими підрозділами.

Держкомтелерадіо вносить до Державного реєстру суб'єктів видавничої справи, що підпадають під такі категорії:

- *видавці* – видавництва, видавничі організації, фізичні особи — суб'єкти підприємницької діяльності, обсяг випуску видавничої продукції яких становить понад 5 назв на рік;

³⁰⁸ Про Державний реєстр видавців, виготівників і розповсюджувачів видавничої продукції: Постанова Кабінету Міністрів України від 28 вересня 1998 р. № 1540.

- *виготівники видавничої продукції* – випускають видавничу продукцію на суму понад 500 тис. гривень на рік;
- *розповсюджувачі видавничої продукції* – оптово-роздрібні книготорговельні підприємства та інші підприємства і організації, які мають мережу книготорговельних підприємств;
- *суб'єкти видавничої справи*, що провадять 2–3 види діяльності у видавничій справі.

Внесення до реєстру решти суб'єктів видавничої справи віднесе-но до компетенції місцевих підрозділів Держкомтелерадіо.

Внесення суб'єктів видавничої справи до Державного реєстру здійснюється на підставі їх заяви. У відповідній заяві про державну реєстрацію зазначаються:

1) засновник (співзасновники), включаючи прізвище, ім'я, по батькові та відповідні паспортні дані (для громадян); повну назву (для юридичної особи); місцезнаходження, номери засобів зв'язку та банківських рахунків;

2) дані про суб'єкта видавничої справи;

3) мови, якими планується випускати чи розповсюджувати видавничу продукцію – державною, російською, іншими мовами національних меншин України (конкретно якими), іноземними мовами (якими);

4) джерела надходження видавничої продукції для розповсюдження – вітчизняні або зарубіжні (з яких країн);

5) джерела фінансового та матеріально-технічного забезпечення діяльності видавців, виготівників і розповсюджувачів видавничої продукції.

До заяви про внесення суб'єкта видавничої справи до Державного реєстру додаються такі документи: 1) нотаріально засвідчена копія свідоцтва про державну реєстрацію юридичної особи чи фізичної особи — суб'єкта підприємницької діяльності; 2) нотаріально засвідчені копії установчих документів (статут, положення, якими передбачено провадження видавничої діяльності, виготовлення та розповсюдження видавничої продукції, установчий договір); 3) передбачувані дані про річний обсяг випуску, виготовлення та розповсюдження видавничої продукції.

Заява про внесення суб'єкта видавничої справи до Державного реєстру розглядається у місячний термін. Після прийняття рішення про внесення до Державного реєстру та сплати реєстраційного збору суб'єктові видавничої справи видається свідоцтво встановленого зразка.

Законодавство визначає також види діяльності у видавничій справі, яка може здійснюватися без внесення до Державного реєстру. Зокрема, такою діяльністю можуть займатися:

- органи законодавчої, виконавчої, судової влади для випуску у світ офіційних видань з матеріалами законодавчого та іншого нормативно-правового характеру;
- підприємства, організації, навчальні заклади, наукові установи, творчі спілки, інші юридичні особи – для випуску у світ і безоплатного розповсюдження інформаційних та рекламних видань.

Закон України “Про видавничу справу” (ст. 6) передбачає надання *державної підтримки* видавничій справі. Відповідно до норм ч. 2 цієї статті, держава надає підтримку видавництвам, видавничим організаціям, поліграфічним та книготорговельним підприємствам, що випускають або розповсюджують не менш як 50% продукції державною мовою та малотиражні (до 5 тис. примірників) видання мовами нечисленних національних меншин, шляхом надання пільг щодо сплати податків та зборів. Ця державна підтримка полягає у звільненні від сплати ПДВ.

Для набуття статусу друкованого видання та можливості розповсюдження продукції видавець має додержувати вимог щодо обов’язкової наявності вихідних відомостей та обов’язкових примірників видань.

Згідно зі ст. 23 Закону України “Про видавничу справу”, *вихідні відомості видання* – це сукупність даних, які характеризують видання і призначені для його оформлення, інформування споживача, бібліографічного опрацювання і статистичного обліку.

Елементами вихідних відомостей є:

- відомості про авторів та інших осіб, які брали участь у створенні видання;
- назва (основна, паралельна, ключова, альтернативна) видання;
- надзаголовкові дані; підзаголовкові дані; вихідні дані;
- випускні дані (номер і дата видачі документа про внесення видавця до Державного реєстру, обсяг видання, тираж тощо);
- класифікаційні індекси;
- міжнародні стандартні номери;
- знак охорони авторського права.

Перелік, зміст і порядок оформлення вихідних відомостей для кожного виду видань визначаються стандартами. Вихід у світ видання без обов’язкових для нього вихідних відомостей не допускається.

Обов'язкові примірники видань – це примірники різних видів тиражованих видань, які надсилаються установам і організаціям відповідно до законодавства України. Перелік установ та організацій, яким надсилається обов'язковий примірник видань, пов'язані з цим права та обов'язки установ і організацій-одержувачів та видавців визначаються Законом України “Про обов'язковий примірник документів”³⁰⁹. Згідно зі ст. 8 цього Закону, видавці зобов'язані доставляти:

- *обов'язковий безоплатний примірник видань* – Книжковій палаті України, національним, у тому числі спеціалізованим, всеукраїнським бібліотекам, Верховній Раді України, Президентові України, Кабінетові Міністрів України, органам виконавчої влади у галузі інформації, на які покладена функція державної реєстрації засобів масової інформації (Мін'юст) та ведення Державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції (Держкомтелерадіо);
- *обов'язковий безоплатний примірник видань, що виготовляються (в тому числі публікуються) на відповідній території* – універсальним бібліотекам (Автономної Республіки Крим та обласним);
- *обов'язковий безоплатний примірник малотиражних документів (до 100 примірників)* – Книжковій палаті України та національним бібліотекам;
- *обов'язковий безоплатний примірник нормативно-правових актів, довідкових, енциклопедичних, історичних та наукових видань у сфері правознавства* – Конституційному Суду України.

Обов'язкові примірники документів доставляються (надсилаються) в день виходу в світ першої частини тиражу.

Важливу роль у веденні обліку друкованих видань відіграє *Книжкова палата України* (ст. 27 Закону України “Про видавничу справу”), яка є державною науковою установою у сфері видавничої справи та інформаційної діяльності, що здійснює державну бібліографічну реєстрацію та централізовану каталогізацію всіх без винятку видів видань, випущених в Україні;

³⁰⁹ Про обов'язковий примірник документів: Закон України від 9 квітня 1999 р. № 595-XIV // Відомості Верховної Ради України. – 1999. – № 22–23. – Ст. 199.

12.4. Інформаційні агентства

Одним із важливих суб'єктів інформаційної діяльності в сфері масової інформації є *інформаційні агентства*. Як правило, саме інформаційні агентства є основним джерелом інформації, що розповсюджується за допомогою друкованих та електронних засобів масової інформації. Відповідно до Закону України “Про інформаційні агентства”³¹⁰ (ст. 1), це *зареєстровані як юридичні особи суб'єкти інформаційної діяльності, що діють з метою надання інформаційних послуг*.

Хоча насправді інформаційні агентства не лише надають інформаційні послуги шляхом поширення інформаційної продукції, а й створюють власні інформаційні продукти. Адже, згідно зі ст. 5 цього Закону, діяльність інформаційних агентств включає такі дії, як: *збирання, обробка, творення, зберігання, підготовка інформації до поширення, випуск та розповсюдження інформаційної продукції*. При чому випуск і розповсюдження інформаційними агентствами власної продукції з метою отримання прибутку з погляду законодавства розглядається як підприємницька діяльність в інформаційній сфері.

Продукція інформаційного агентства – це матеріалізований результат його діяльності, призначений для розповсюдження з метою задоволення інформаційних потреб громадян, юридичних осіб, держави, і, як правило, є власністю агенства. Основними видами продукції інформаційних агентств є: електронна, друкована, фото-, кіно-, аудіо- та відеопродукція.

Продукція інформаційних агентств *розповсюджується за допомогою засобів комунікації*, до яких законодавство відносить: друковані та екранні видання, радіо, телебачення (кабельне, супутникове, глобальне), електричний та електронний зв'язок (телеграф, телефон, телекс, телефакс), комп'ютерні мережі та інші телекомунікації.

Інформаційне агентство може бути створене у будь-якій організаційній формі та має статус юридичної особи, якого набуває з моменту його державної реєстрації. Мета, завдання, функції та порядок діяльності інформаційного агентства визначаються законодавством та його статутом або положенням, яке затверджується засновником або співзасновниками інформаційного агентства.

³¹⁰ Про інформаційні агентства: Закон України від 28 лютого 1995 р. № 74/95-ВР // Відомості Верховної Ради України. – 1995. – № 13. – Ст. 83.

До основних суб'єктів діяльності інформаційних агентств законодавство, зокрема, відносить таких як:

- *засновник (співзасновники) інформаційного агентства;*
- *керівник інформаційного агентства* – особа, яка безпосередньо керує всіма підрозділами інформаційного агентства, відповідає за результати його роботи, підписує фінансові документи і виконує іншу роботу згідно з наданими йому засновником (співзасновниками) інформаційного агентства повноваженнями;
- *журналіст інформаційного агентства* – творчий працівник, який збирає, одержує, створює та готує інформацію для інформаційного агентства і діє від його імені на підставі трудових чи інших договірних відносин з ним або за його уповноваженням.
- *спеціаліст у галузі засобів комунікації* – працівник інформаційного агентства, який на професійних засадах здійснює розповсюдження інформаційної продукції через засоби комунікації та несе відповідальність за використання цих засобів виключно на підставі чинного законодавства України.
- *видавець (виробник) продукції інформаційного агентства* – саме агентство або суб'єкт підприємництва, який здійснює випуск (тиражування або виробництво) інформаційної продукції на підставі угоди, укладеної між ним та інформаційним агентством;
- *розповсюджувач продукції інформаційного агентства* – саме агентство або суб'єкт підприємництва – власник (користувач) засобу комунікації, через який він розповсюджує продукцію інформаційного агентства в порядку і на умовах, визначених чинним законодавством України та укладеною між ними угодою;
- *споживач продукції інформаційного агентства* – громадяни, юридичні особи, державні органи України та інших держав, які на підставі відповідної угоди з інформаційними агентствами одержують їх інформаційну продукцію.

Однією з основних відмінностей інформаційних агентств від засобів масової інформації є специфіка відносин між агентством та споживачами його інформаційної продукції, яка надається останнім на підставі раніше укладеної угоди. На відміну від цього продукція ЗМІ, як правило, поширюється для невизначеної кількості споживачів.

Згідно зі ст. 9 Закону України “Про інформаційні агентства” *право на заснування інформаційного агентства в Україні належить громадянам та юридичним особам України.*

Іноземці та іноземні юридичні особи мають право бути лише співзасновниками інформаційних агентств України. При цьому сукупна частка іноземних співзасновників у статутному фонді інформаційного агентства не може становити більш як 35%.

Залежно від форми власності інформаційні агентства можуть бути *державними або недержавними.*

Іноземні інформаційні агентства мають право діяти на території України лише шляхом відкриття своїх *представництв*, які представляють зареєстровану в Україні відповідно до чинного законодавства як суб’єкт інформаційної діяльності будь-яку установу (бюро, представництво, корпункт тощо), що представляє в Україні державне або недержавне інформаційне агентство, зареєстроване як юридична особа згідно з чинним законодавством відповідної країни.

Державну реєстрацію інформаційних агентств в Україні здійснює Міністерство юстиції України³¹¹, а представництв іноземних інформаційних агентств – Міністерство закордонних справ України.

У заяві про державну реєстрацію інформаційного агентства мають бути зазначені:

- 1) засновник (співзасновники) реквізитів;
- 2) повне найменування та назва інформаційного агентства;
- 3) вид інформаційного агентства та його організаційно-правова форма;
- 4) передбачувана сфера розповсюдження інформаційної продукції (місцева, регіональна, національна, національна та зарубіжна, зарубіжна);
- 5) мови, якими буде розповсюджуватися інформаційна продукція;
- 6) програмна мета та основні напрями діяльності інформаційного агентства;
- 7) джерела фінансового та матеріально-технічного забезпечення діяльності інформаційного агентства;
- 8) місцезнаходження інформаційного агентства.

До заяви про державну реєстрацію інформаційних агентств як суб’єктів підприємницької діяльності додаються відповідні установчі документи.

³¹¹ Про затвердження Положення про державну реєстрацію інформаційних агентств як суб’єктів інформаційної діяльності: Наказ Міністерства юстиції України від 21 лютого 2006 р. № 12/5.

Заяву про державну реєстрацію інформаційного агентства розглядає Мін'юст у семиденний термін з дня її одержання.

Підставами для відмови у державній реєстрації інформаційного агентства є випадки, коли:

- назва інформаційного агентства, його програмна мета, основні цілі та напрями діяльності суперечать законодавству України;
- реєструючим органом уже зареєстровано інше інформаційне агентство з тією ж назвою;
- заяву подано до закінчення року з дня набрання законної сили рішенням суду про припинення діяльності цього інформаційного агентства.

З метою забезпечення законності в діяльності інформаційних агентств та можливості ідентифікації інформації, що розповсюджується Законом України “Про інформаційні агентства” (ст. 28) встановлено вимоги щодо обов’язкової наявності *вихідних даних продукції інформаційних агентств*. Відповідно до цих вимог кожен випуск продукції інформаційних агентств повинен містити такі вихідні дані:

- 1) назву інформаційного агентства;
- 2) прізвище чергового редактора чи відповідального за випуск та їх реквізити;
- 3) порядковий номер випуску і дату його виходу у світ;
- 4) адресу агентства.

При розповсюдженні своєї продукції інформаційні агентства мають переважне право на використання засобів комунікації. Державним інформаційним агентствам надається першочергове право перед іншими інформаційними агентствами на використання засобів комунікації для розповсюдження інформації, яка має особливе значення для держави і суспільства.

12.5. Правові основи діяльності електронних ЗМІ

Нині найважливішу роль у сфері масової інформації відіграє діяльність електронних засобів масової інформації, до яких належать телебачення і радіомовлення. Як уже зазначалося, особливості правового регулювання їх діяльності зумовлені використанням ними технічних засобів розповсюдження інформації, а для ефірних ЗМІ – ще й використанням такого вичерпного ресурсу, як радіочастотний, що потребує додаткового впорядкування їх діяльності.

Існують певні міжнародно-правові стандарти діяльності електронних ЗМІ, які охоплюють не лише технічну сторону (міжнародно-правове регулювання використання радіочастотного ресурсу), а й певною мірою змістов.

Необхідність певною мірою регулювати змістові аспекти діяльності електронних ЗМІ пояснюється незалежністю розповсюдження їх інформації від державних кордонів і, отже, неможливістю національної держави встановлювати правила розповсюдження інформації на власній території закордонними електронними ЗМІ. Наприклад, можна назвати прийняту ЮНЕСКО Декларацію керівних принципів щодо використання мовлення через супутники для вільного використання інформації, розвитку освіти і розширення культурних обмінів, яка містить низку норм, що спрямовані на вирішення подібних питань, зокрема:

- ч. 1 ст. 2 цієї Декларації передбачає, що “при мовленні через супутники повинні поважатися суверенітет та рівність усіх держав”;
- ст. 10 установлює, що “при підготовці програм прямого мовлення на інші країни потрібно враховувати розбіжності в національних законах країн, об’єктів мовлення”;
- ст. 11 визначає, що “принципи цієї Декларації повинні застосовуватися з повною повагою до прав людини і основних свобод”³¹².

Питанням регулювання діяльності організації телевізійного мовлення, що розповсюджується на іноземні країни, присвячена також і підписана Україною 14 червня 1996 р. Європейська конвенція про транскордонне телебачення³¹³, процес ратифікації якої нашою державою, на жаль, затягнувся.

Основним національним нормативно-правовим актом у цій галузі є Закон України “Про телебачення і радіомовлення”³¹⁴.

Згідно із ст. 1 цього Закону, *телерадіомовлення – це створення (комплектування та/або пакетування) і розповсюдження програм, пакетів програм, передач з використанням технічних засобів телекомунікацій для публічного приймання за допомогою побутових теле-*

³¹² Декларация руководящих принципов по использованию вещания через спутники для свободного распространения информации, развития образования и расширения культурных обменов от 15 ноября 1972 года

³¹³ Рада Європи. Європейська конвенція про транскордонне телебачення ETS № 132. Страсбург. 5 травня 1989 р.

³¹⁴ Про телебачення і радіомовлення: Закон України від 21 грудня 1993 р. № 3759-XII // Відомості Верховної Ради України. – 1994. – № 10. – Ст. 43.

та радіоприймачів у відкритий спосіб чи за абонентну плату на договірних засадах.

Суб'єктом телерадіомовлення є *телерадіоорганізація* – зареєстрована у встановленому законодавством порядку юридична особа, яка на підставі виданої Національною радою України з питань телебачення і радіомовлення ліцензії на мовлення створює або комплектує та/чи пакетує телерадіопрограми і/або передачі та розповсюджує їх за допомогою технічних засобів мовлення.

Законодавство виділяє такі види телеорганізацій: *приватні, державні, комунальні, громадські та Суспільне телерадіомовлення:*

- *приватні телерадіоорганізації* – це такі, що перебувають у власності фізичних або юридичних осіб, які набули права власності на телерадіоорганізацію або на частку її статутного фонду шляхом заснування або в інший передбачений законодавством спосіб;
- *державні телерадіоорганізації* – телерадіоорганізації, які є державними підприємствами і засновані органами державної влади;
- *комунальні телерадіоорганізації* – телерадіоорганізації, які належать територіальним громадам і засновані органами місцевого самоврядування;
- *громадські телерадіоорганізації* – телерадіоорганізації, які відповідно до закону є неприбутковими організаціями, створеними з метою задоволення інформаційних потреб територіальних громад.

Суспільне телерадіомовлення – телерадіоорганізація зі статусом єдиної загальнонаціональної неподільної і неприбуткової системи масової комунікації, яка є об'єктом права власності Українського народу і діє згідно з єдиною програмною концепцією. Порядок створення та діяльності суспільного телерадіомовлення визначається Законом України “Про систему Суспільного телебачення і радіомовлення України”³¹⁵.

Згідно зі нормами ст. 12 Закону України “Про телебачення і радіомовлення”, право на заснування телерадіоорганізацій як суб'єктів господарювання в Україні належить юридичним особам України та громадянам України, не обмеженим у цивільній дієздатності.

³¹⁵ Про систему Суспільного телебачення і радіомовлення України: Закон України // Відомості Верховної Ради України. – 1997. – № 45. – Ст. 284.

Не можуть бути засновниками телерадіоорганізацій:

- органи державної влади та органи місцевого самоврядування, якщо рішення про їх створення або положення про них не передбачає повноважень засновувати телерадіоорганізації;
- юридичні особи, статутні документи яких не передбачають можливість створення телерадіоорганізацій;
- іноземні юридичні і фізичні особи та особи без громадянства;
- політичні партії, профспілкові, релігійні організації та юридичні особи, яких вони заснували;
- громадяни, які за вироком суду відбувають покарання у місцях позбавлення волі або визнані судом недієздатними.

Допускається участь іноземних фізичних або юридичних осіб у статутному фонді телерадіоорганізацій.

Органом державного регулювання у сфері телебачення і радіомовлення є **Національна рада України з питань телебачення і радіомовлення** – орган, порядок призначення персонального складу якого прямо передбачений Конституцією України.

Правовий статус і компетенція Національної ради України з питань телебачення і радіомовлення визначаються Законом України “Про Національну раду України з питань телебачення і радіомовлення”³¹⁶ Згідно зі ст. 1 цього Закону *Національна рада України з питань телебачення і радіомовлення (Національна рада) є конституційним, постійно діючим колегіальним органом, метою діяльності якого є нагляд за дотриманням законів України у сфері телерадіомовлення, а також здійснення регуляторних повноважень, передбачених цими законами.*

У склад Національної ради складає вісім осіб, по чотири з яких призначаються відповідно Верховною Радою України і Президентом України строком на чотири роки. Одна й та сама особа може бути повторно призначена членом Національної ради лише один раз. Національна рада є повноважною у разі призначення не менше як шість її членів.

Повноваження Національної ради, згідно із Законом “Про Національну раду України з питань телебачення і радіомовлення” поділяються на регуляторні (ст. 14) та наглядові (ст. 13).

До *регуляторних повноважень*, що здійснюються Національною радою у сфері телерадіомовлення, зокрема, належать:

³¹⁶ Про Національну раду України з питань телебачення і радіомовлення: Закон України від 23 вересня 1997 р. № 538/97-ВР // Відомості Верховної Ради України. – 1997. – № 48. – Ст. 296.

- ліцензування телерадіомовлення;
- участь у розробці та погодження проекту Національної таблиці розподілу смуг радіочастот України і Плану використання радіочастотного ресурсу України у частині смуг радіочастот, виділених для потреб телерадіомовлення;
- розробка умов використання та визначення користувачів радіочастотного ресурсу, виділеного для потреб телерадіомовлення;
- забезпечення і сприяння конкуренції у діяльності телерадіоорганізацій усіх форм власності відповідно до вимог законодавства, створення умов щодо недопущення усунення, обмеження чи спотворення конкуренції у телерадіоінформаційному просторі;
- ведення Державного реєстру телерадіоорганізацій України.

У рамках своїх *наглядових повноважень* Національна рада, зокрема, здійснює:

- нагляд за дотриманням ліцензіатами вимог законодавства України у сфері телебачення і радіомовлення;
- нагляд за дотриманням ліцензіатами вимог законодавства України щодо реклами та спонсорства у сфері телерадіомовлення;
- нагляд за дотриманням ліцензіатами ліцензійних умов та умов ліцензій;
- нагляд за дотриманням ліцензіатами визначеного законодавством порядку мовлення під час проведення виборчих кампаній та референдумів;
- нагляд за дотриманням стандартів та норм технічної якості телерадіопрограм;
- нагляд за дотриманням телерадіоорганізаціями законодавства України у сфері кінематографії;
- нагляд за дотриманням телерадіоорганізаціями вимог законодавства України щодо частки вітчизняного продукту у їх програмах (передачах) та щодо вживання мов при здійсненні телерадіомовлення;
- нагляд за дотриманням телерадіоорганізаціями законодавства у сфері захисту суспільної моралі;
- нагляд за дотриманням телерадіоорганізаціями вимог законодавства щодо частки іноземних інвестицій у їх статутному фонді;
- застосування в межах своїх повноважень санкцій відповідно до закону;
- офіційний моніторинг телерадіопрограм.

Частину функцій Національної ради здійснюють *Представники Національної ради* в Автономній Республіці Крим, областях, містах Києві та Севастополі, до компетенції яких (ст. 11) віднесено:

- нагляд за дотриманням ліцензіатами вимог законодавства у галузі телерадіомовлення;
- нагляд за виконанням ліцензіатами ліцензійних умов та умов ліцензії;
- моніторинг телерадіопрограм;
- нагляд за дотриманням ліцензіатами визначеного законодавством порядку мовлення під час проведення виборчих кампаній та референдумів, інформування Центральної виборчої комісії, відповідних територіальних виборчих комісій, Національної ради про виявлені порушення;
- надсилання до Національної ради подання про факти порушень законодавства у галузі телерадіомовлення.

Цим же Законом (ст. 21) визначено перелік санкцій, які Національна рада може застосовувати до телерадіорганізацій (ліцензіатів) у разі порушення ними законодавства України, ліцензійних умов та умов ліцензії. У таких випадках Національна рада має право:

- оголошувати попередження;
- накладати штраф;
- звертатися до суду із заявою про анулювання ліцензії.

Єдиним і достатнім документом, що надає ліцензіату право відповідно до умов ліцензії здійснювати мовлення, користуватися каналами мовлення за умови наявності у володільців радіоелектронних засобів передбачених законом дозволів на їх експлуатацію є *ліцензія на мовлення*, видана Національною радою

Телерадіорганізація-ліцензіант має право розпочати мовлення протягом року з дня набрання чинності відповідною ліцензією, про що в десятиденний термін зобов'язана повідомити Національну раду.

Ліцензуванню підлягають такі види мовлення: 1) супутникове; 2) ефірне; 3) кабельне; 4) проводове; 5) багатоканальне.

Видача ліцензій на мовлення здійснюється:

- *на конкурсних засадах* (за результатами відкритих конкурсів) для ефірного та багатоканального мовлення з використанням радіочастотного ресурсу;
- *без конкурсів* (за заявковим принципом) щодо всіх інших видів мовлення.

Конкурс на отримання ліцензії оголошується Національною радою, причому в оголошенні зазначаються територія розповсюдження, канал та частоти, потужність передавача, обсяг мовлення (годин на добу) тощо.

Національна рада визначає також конкурсні умови, а саме:

- ліцензійні умови для відповідного виду мовлення;
- вимоги до програмної концепції мовлення;
- вимоги щодо організаційно-технічних, фінансових та інвестиційних зобов'язань майбутнього ліцензіата.

Безпосередній перелік таких умов визначається Рішенням Національної ради³¹⁷. Рішення про видачу ліцензії приймається Національною радою після визначення переможця конкурсного відбору і оформляється протоколом, який підписується під час засідання Національної ради. Строк дії ліцензії встановлюється рішенням Національної ради згідно із заявою телерадіоорганізації, але він не може бути меншим за 7 років – для ефірного мовлення і 10 років – для кабельного (проводового) мовлення. Після закінчення визначеного строку ліцензія втрачає чинність, якщо не прийнято рішення про її продовження.

У *ліцензії* Національної ради, зокрема, зазначаються: назва та вид телерадіоорганізації, місцезнаходження, вид діяльності, логотипи та позивні, програмна концепція, територія і спосіб розповсюдження, категорія споживачів, мова програм і передач (із зазначенням відсоткової частки української мови), інформація про засновників.

Інструментом, що забезпечує можливість належної ідентифікації програм та передач і здійснення контролю за додержанням законодавства та ліцензійних умов, є обов'язок телерадіоорганізацій повідомляти *вихідні дані* (ст. 46 Закону України “Про телебачення і радіомовлення”). До вихідних даних належать:

- під час трансляції (ретрансляції) радіопрограми – *найменування та позивні* телерадіоорганізації, які вона повинна повідомляти не рідше ніж щогодини;
- під час трансляції телепередачі – логотип, емблема або інші вихідні дані, які повинні постійно використовуватись.

Крім того, для трансляції телепередач Рішенням Національної ради запроваджено Систему візуальних позначок класифікації кіно-

³¹⁷ Про затвердження конкурсних умов: Рішення Національної ради України з питань телебачення і радіомовлення від 21 березня 2007 р. № 350.

відеопродукції залежно від аудиторії, на яку вона розрахована³¹⁸. Відповідно до цієї Системи, кіновідеопродукція, що транслюється на телеканалах України, поділяється на три категорії, залежно від аудиторії, на яку вона розрахована. Її показ по телебаченню має супроводжуватися відповідними візуальними позначками:

категорія I – без обмежень аудиторії (загальнодоступна) – зелений колір;

категорія II – перегляд неповнолітніми глядачами рекомендується разом з батьками або з одним із батьків – жовтий колір;

категорія III – рекомендується тільки для дорослих – червоний колір.

Фільми, заборонені для розповсюдження і демонстрування в Україні та без права показу на телеканалах, не підпадають під жодну категорію.

Під час трансляції візуальна позначка на телеекрані кіновідеопродукції категорій II і III має постійно бути у правому нижньому куті.

Кіновідеопродукція, що належить до категорії I, супроводжується відповідною позначкою на телеекранах протягом перших трьох хвилин трансляції.

Телекомпанії зобов'язані подавати візуальні позначки категорій II (трикутник) і III (квадрат) у друкованих програмах своїх передач.

12.6. Розповсюдження і демонстрування фільмів

Значна частина розповсюджуваної візуальної масової інформації подається у вигляді кінофільмів та відеофільмів. Закон України “Про кінематографію” (ст. 1) визначає *фільм як аудіовізуальний твір кінематографії, що складається з епізодів, поєднаних між собою творчим задумом і зображувальними засобами, та який є результатом спільної діяльності його авторів, виконавців і виробників*.

Загалом, кінематографія, розглядається законодавством як галузь культури, що по'єднує комплекс видів професійної діяльності, пов'язаної з виробництвом, розповсюдженням, зберіганням та демонструванням фільмів, навчально-науковою роботою у цій галузі. Але серед напрямів діяльності в галузі кінематографії можна виділити два, безпосередньо пов'язаних з розповсюдженням аудіовізу-

³¹⁸ Про затвердження системи візуальних позначок класифікації кіновідеопродукції залежно від аудиторії, на яку вона розрахована: Рішення Національної ради України з питань телебачення і радіомовлення від 18 червня 2003 р. № 781.

альної інформації. До них належать розповсюдження та демонстрування фільмів.

Розповсюдження (прокат) фільму – це виготовлення фільмокопій (тиражування), продаж і передача їх у прокат юридичним та фізичним особам. Суб'єктами діяльності щодо розповсюдження фільмів є: виробники, дистриб'ютори (прокатники) фільмів, кінокопіювальні підприємства, фонди фільмів, архіви кіно-, фото-, фонодокументів тощо.

Демонстрування (публічний показ, публічне сповіщення і публічна демонстрація) фільму – це професійна кінематографічна діяльність, що полягає в показі фільму глядачам у призначених для цього приміщеннях (кінотеатрах, інших кіновидовищних закладах), на відеоустановках, а також каналами мовлення телебачення. Суб'єктами діяльності щодо демонстрування фільмів є: кінотеатри, кіноустановки, відеоустановки, канали мовлення телебачення (ефірного, кабельного, ефірно-кабельного, супутникового тощо).

Державне регулювання діяльності з розповсюдження та демонстрування фільмів забезпечується шляхом:

- установлення загальнобов'язкових технічних стандартів, норм та правил розповсюдження і демонстрування фільмів;
- ведення Державного реєстру виробників, розповсюджувачів і демонстраторів фільмів;
- надання права на демонстрування та розповсюдження фільмів у дозвільному порядку.

Органом державного регулювання в галузі кінематографії є **Міністерство культури і туризму України**³¹⁹ (МКТ), у структурі якого діють Державна служба кінематографії та Експертна комісія МКТ з питань розповсюдження і демонстрування фільмів.

У рамках своєї регуляторної діяльності в галузі кінематографії, Мінкультури встановлює вже згадані *технічні стандарти, норми та правила розповсюдження і демонстрування фільмів*, дотримання яких є обов'язковим для суб'єктів кінематографії незалежно від форм власності. Крім того, згідно зі ст. 14 Закону України “Про кінематографію”, іноземні фільми перед розповсюдженням в Україні в обов'язковому порядку повинні бути дубльовані або озвучені чи субтитровані державною мовою, вони також можуть бути дубльовані або озвучені чи субтитровані мовами національних меншин.

³¹⁹ Про затвердження Положення про Міністерство культури і туризму України: Постанова Кабінету Міністрів України від 8 листопада 2006 р. № 1566.

Основні функції регулювання діяльності у сфері кінематографії виконує Державна служба кінематографії (Держкіно), яка є урядовим органом державного управління, що діє у складі МКТ і підпорядковується йому³²⁰.

Основними завданнями Держкіно є:

- сприяння відродженню національної кінематографії, посилення її впливу на формування духовних цінностей Українського народу, створення належних правових і економічних умов для розвитку національного кіномистецтва та конкурентоспроможної на міжнародному ринку кіноіндустрії;
- участь у межах своєї компетенції у реалізації державної політики в галузі кінематографії;
- координація роботи місцевих органів виконавчої влади з питань реалізації державної політики у галузі кінематографії.

Зокрема, в рамках виконання своїх повноважень Держкіно:

- веде Державний реєстр виробників, розповсюджувачів і демонстраторів фільмів;
- видає державні посвідчення на право розповсюдження і демонстрування фільмів.

Порядок ведення *Державного реєстру виробників, розповсюджувачів і демонстраторів фільмів* визначається відповідним Положенням, затверджене Кабінетом Міністрів України³²¹.

Одним із головних завдань ведення цього Реєстру є ідентифікація суб'єктів кінематографії, що здійснюють виробництво, розповсюдження і демонстрування фільмів на професійній основі з дотриманням технічних стандартів, норм та правил у цій сфері.

Реєстр складається з трьох розділів: виробники фільмів, розповсюджувачі фільмів, демонстратори фільмів, у яких відображаються дані:

- про виробництво фільмів на власній або найманій (орендованій) виробничій базі з повним технологічним циклом для виготовлення оригіналів фільмових матеріалів на кіноплівці, магнітних чи інших електронних носіях – для виробників фільмів;
- про отримання права на виготовлення фільмокопій на кіноплівці, магнітних чи інших електронних носіях, продаж та передачу їх у прокат для демонстрування і для приватного (у домаш-

³²⁰ Питання Державної служби кінематографії: Постанова Кабінету Міністрів України від 7 березня 2006 р. № 251.

³²¹ Про затвердження Положення про Державний реєстр виробників, розповсюджувачів і демонстраторів фільмів: Постанова Кабінету Міністрів України від 14 січня . 2004 р. № 27.

ніх умовах) перегляду; про умови виготовлення фільмокопій: на власній або найманій (орендованій) виробничій базі – для розповсюджувачів фільмів;

- про демонстрування фільмів у призначених для цього приміщеннях – для демонстраторів фільмів.

Внесення суб'єкта кінематографії до Реєстра здійснюється на підставі відповідної заяви, яка розглядається в місячний термін з дня отримання її реєструючим органом. За результатами розгляду заяви орган управління кінематографією ухвалює рішення про внесення до Реєстру суб'єкта кінематографії чи про відмову у внесенні до Реєстру. При внесенні суб'єкта кінематографії до Реєстру йому видають свідоцтво встановленого зразка.

Рішення про внесення до Реєстру суб'єкта кінематографії та видачу йому свідоцтва ухвалюють:

- Держкіно – стосовно виробників фільмів; розповсюджувачів фільмів, які отримали право на розповсюдження фільмів на всій території України;
- місцеві органи управління кінематографією – стосовно розповсюджувачів фільмів, які отримали право на розповсюдження фільмів у межах відповідних адміністративно-територіальних одиниць; демонстраторів фільмів, які проводять свою діяльність у межах відповідних адміністративно-територіальних одиниць.

Одним із ключових засобів регулювання розповсюдження і демонстрування на території України всіх видів вітчизняних та іноземних фільмів є видача *Державного посвідчення на право розповсюдження і демонстрування фільмів (Прокатного посвідчення)*. Прокатне посвідчення є документом, що засвідчує відповідне право та визначає умови розповсюдження і демонстрування фільмів. Фільми, на які видані державні посвідчення на право розповсюдження і демонстрування, вносяться до Державного реєстру фільмів³²².

Безпосередньо порядок видачі прокатних посвідчень визначається Положенням про державне посвідчення на право розповсюдження і демонстрування фільмів, затверджене Постановою Кабінету Міністрів України³²³.

³²² Про затвердження Положення про державну реєстрацію фільмів: Наказ Мінкультури від 31 серпня 2004 р. № 571.

³²³ Про затвердження Положення про державне посвідчення на право розповсюдження і демонстрування фільмів: Постанова Кабінету Міністрів України від 17 серпня 1998 р. № 1315.

Прокатне посвідчення дає право розповсюджувати і демонструвати на території України всі види фільмів, вироблених в Україні та за її межами, будь-яким кінотеатрам, кіноустановкам, відеоустановкам, прокатним пунктам відеокасет, торговельним підприємствам, підприємствам з тиражування, а також телеорганізаціям, у тому числі кабельному телебаченню, незалежно від форми власності.

Згідно з цим Положенням (п. 2), Прокатне посвідчення може засвідчувати два види прав: право розповсюдження фільму та право демонстрування фільму.

Право розповсюдження фільму є виключним (ексклюзивним) або невиключним (неексклюзивним) правом на тиражування, продаж, передавання в прокат, оренду фільму. Це право складається з:

- *кінотеатрального права* (тиражування фільмокопій на кіноплівці, передавання їх у прокат, оренду);
- *права домашнього відео* (тиражування фільмокопій на відеоносіях, їх продаж, передавання в прокат);
- *права публічного комерційного відео* (тиражування фільмокопій на відеоносіях, їх продаж, передавання в прокат, оренду для публічного показу через відеопроєкцію);
- *телевізійного права* (тиражування фільмокопій на відеоносіях, їх продаж, передавання в прокат для публічного показу каналами мовлення телебачення);

Право демонстрування фільму – це виключне (ексклюзивне) або невиключне (неексклюзивне) право на демонстрування (публічний показ) фільму. Це право складається з:

- *кінотеатрального права* (демонстрування фільмокопій на кіноплівці у призначених для цього приміщеннях: кінотеатрах, кіноустановках);
- *права публічного комерційного відео* (демонстрування фільмокопій на відеоносії у призначених для цього та обладнаних спеціальною відеопроєкційною апаратурою приміщеннях або у приміщеннях, безпосередньо не пов'язаних з демонструванням фільмів, обладнаних відеопроєкційною апаратурою або телевізійними приймачами);
- *телевізійного права* (демонстрування фільмокопій на відеоносії або кіноплівці каналами мовлення ефірного, супутникового, кабельного телебачення платного чи безоплатного).

Прокатне посвідчення видається юридичній або фізичній особі, яка відповідно до законодавства є суб'єктом підприємницької діяльності. Рішення про видачу посвідчення приймає Держкіно на підставі відповідної заяви.

Прокатне посвідчення видається:

- власникам кінотеатрального права – на кожний фільм і кожному фільмокопію на кіноплівці;
- власникам телевізійного права, права домашнього відео та публічного комерційного відео – на кожний фільм або кілька фільмів.

Для одержання прокатного посвідчення власник відповідних прав на фільм подає до Держкіно:

- заяву про видачу прокатного посвідчення, в якій зазначаються назва фільму мовою оригіналу та українською мовою, країна і студія-виробник, рік випуску;
- нотаріально засвідчені копії (ксерокопії) угод (контрактів, договорів), інших документів, які підтверджують право даної особи на розповсюдження і демонстрування фільму, починаючи від першого власника майнових авторських прав;

в) коротку анотацію фільму, довідку про основний творчий склад знімальної групи та про метраж і тривалість фільму, засвідчені підписом власника відповідних прав на фільм;

г) фільмокопію на кіноплівці або інших носіях, яка відповідає технічним вимогам для перегляду, дубльована (озвучена, субтитрована) українською мовою.

Розгляд заяви, ухвалення рішення щодо державної реєстрації фільму або відмови у ній та видача прокатного посвідчення здійснюються протягом 15 днів. У разі позитивного рішення Держкіно реєструє фільм у Державному реєстрі фільмів, присвоює кожному фільму державний реєстраційний номер та видає прокатне посвідчення. Під час реєстрації також встановлюється *індекс розповсюдження і демонстрації* та визначається *глядацька аудиторія фільма*.

У разі виникнення розбіжностей щодо визначення індексу фільму за згодою власника відповідних прав на фільм цей індекс визначає *Експертна комісія з питань розповсюдження і демонстрування фільмів при Держкіно*, до складу якої входять незалежні експерти – кінознавці, кінокритики, мистецтвознавці, психологи, а також представ-

ники заінтересованих міністерств та інших центральних органів виконавчої влади.

Підставами для *відмови* у державній реєстрації фільму та видачі прокатного посвідчення є:

- висновок експертної комісії щодо невідповідності фільму вимогам Закону України “Про захист суспільної моралі”;
- якщо фільм не дубльований (озвучений, субтитрований) українською мовою на фільмокопії мови оригіналу.

Відмова у державній реєстрації та видачі прокатного посвідчення означає заборону демонстрації та розповсюдження фільму на території України.

Положенням про державне посвідчення на право розповсюдження і демонстрування фільмів встановлені такі *індекси що визначають глядацьку аудиторію та відповідно до неї умови розповсюдження і демонстрування фільмів*, які зазначаються у прокатному посвідченні.

Для фільмів, що не мають обмеження глядацької аудиторії встановлюються індекси: “ДА” – дитяча аудиторія та “ЗА” – загальна аудиторія.

Для фільмів, що мають обмеження глядацької аудиторії:

“14” – фільм, перегляд якого дозволяється дітям до 14 років тільки у супроводі батьків. Самостійний перегляд дітям до 14 років забороняється;

“16” – фільм, перегляд якого забороняється особам віком до 16 років;

“18” – фільм, перегляд якого забороняється особам віком до 18 років;

“Х21” – фільм, перегляд якого забороняється особам віком до 21 року.

Відповідно до встановлених індексів, фільми, що мають обмеження глядацької аудиторії, розповсюджуються і демонструються з дотриманням певних вимог та обмежень. Так, продаж, передання в прокат населенню примірників фільмів на відеоносіях здійснюються з дотриманням таких вимог:

- наявність на відеоносіях інформації про індекс фільму, який визначає глядацьку аудиторію;
- обов’язкове попередженням споживача про встановлені обмеження.

При демонструванні фільмів кінотеатрами і кіновідеоустановками встановлено вимоги щодо *попередження глядача про встановлені об-*

меження та дотримання встановленого часу демонстрування фільму.

Згідно з часовими обмеженнями фільми з індексом обмеження глядацької аудиторії можуть демонструватися:

“14” – на будь-яких сеансах, крім спеціальних дитячих;

“16” – на будь-яких сеансах, крім спеціальних дитячих;

“18” та “X21” – на вечірніх сеансах з 18 години.

При демонструванні фільмів телеорганізаціями необхідно дотримувати таких вимог: *попередження про встановлені обмеження у програмах телепередач; попередження перед початком демонстрування фільму; застосування візуальних позначок класифікації відеопродукції; додержання встановленого часу демонстрування фільму.*

Згідно з часовими обмеженнями фільми з індексом обмеження глядацької аудиторії можуть демонструватися на телебаченні:

“14” – з 18 до 6 години;

“16” – з 21 до 6 години;

“18” – з 23 до 6 години;

“X21” – з 24 до 6 години.

Ще однією вимогою до ідентифікації при демонструванні кінофільмів є встановлена ст. 13 Закону України “Про кінематографію” обов’язковість наявності *вихідних даних (титрів) фільму*, які повинні розміщуватися на матеріальних носіях на початку або в кінці фільму та підлягають обов’язковому відтворенню на всіх фільмокопіях.

У вихідних даних (титрах) у довільній послідовності зазначаються назва фільму, учасники його створення, знак охорони авторського права, рік його створення. За погодженням із власником, який має виключне право на фільм, у вихідні дані (титри) фільму можуть бути внесені додаткові відомості про учасників його створення.

ПРОГРАМА КУРСУ “ІНФОРМАЦІЙНЕ ПРАВО”

І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Предметом курсу “Інформаційне право” є правові відносини щодо інформації, які виникають у сфері здійснення інформаційної діяльності, створення інформаційних продуктів та надання інформаційних послуг.

Цілі і завдання курсу. Вивчаючи курс “Інформаційне право”, студент повинен оволодіти комплексом знань та вмінь, зокрема:

студент повинен знати: основні поняття та категорії інформаційного права; чинне національне законодавство щодо інформаційної сфери; основні міжнародно-правові акти, що регулюють питання інформаційної діяльності; систему та компетенцію органів державної влади що здійснюють управління інформаційною сферою; ключові аспекти інформатизації управлінського процесу;

студент повинен вміти: використовувати норми та принципи національного і міжнародного права стосовно сфери інформаційних правовідносин; здійснювати юридичне забезпечення інформаційної діяльності та надання інформаційних послуг; брати участь в інформаційній діяльності органів державної влади та місцевого самоврядування.

Методична структура курсу. Вивчення положень курсу “Інформаційне право” здійснюється у формі читання лекцій із наступною перевіркою та закріпленням теоретичного матеріалу на практичних заняттях.

Мета лекції – формування теоретичної і методологічної бази для поступового засвоєння основних положень курсу. Інколи лекція є основним джерелом інформації: якщо деякі теми або питання не відображено в підручниках і навчальних посібниках; якщо сталися зміни в законодавстві, якщо окремі теми або питання є складними для засвоєння за самостійного вивчення.

Практичне заняття – одна з основних форм закріплення набутих знань шляхом виконання практичних вправ, вирішенню запропонованих завдань.

Безумовно, важливою є *самостійна робота* студентів, у рамках якої вони повинні детально ознайомитися з нормативно-правовим матеріалом та рекомендованою літературою, підготувати запропоновані теми рефератів і доповідей.

Формою підсумкового контролю є *іспит*.

ІІ. НАВЧАЛЬНИЙ ПЛАН КУРСУ “ІНФОРМАЦІЙНЕ ПРАВО”

№ з/п	Назва теми	Аудиторні заняття			Самостійна робота	Загалом
		усього	лекції	практичні		
1	Основні поняття і категорії інформаційного права	4	2	2	X	4
2	Предмет, метод і система інформаційного права	4	2	2	X	4
3	Гарантії прав і свобод людини у сфері інформації	4	2	2	X	4
4	Основні напрями реалізації прав і свобод людини у сфері інформації	4	2	2	2	6
5	Правові основи інформаційної безпеки	8	4	4	X	8
6	Правові режими інформації та інформаційних ресурсів	4	2	2	X	4
7	Державна таємниця	4	2	2	X	4
8	Конфіденційна інформація	4	2	2	X	4
9	Правові основи захисту інформації	4	2	2	X	4
10	Правове регулювання засобів телекомунікації	8	4	4	2	10
11	Правове регулювання функціонування Інтернет	4	2	2	2	6
12	Правове регулювання діяльності друкованих ЗМІ та інформаційних агентств	4	2	2	2	6
13	Правове регулювання діяльності електронних ЗМІ	4	2	2	2	6
14	Правове регулювання бібліотечної та архівної справи	X	X	X	10	10
15	Інформаційне забезпечення управлінської діяльності	X	X	X	10	10
Разом		60	30	30	30	90

ІІІ. ТЕМАТИЧНИЙ ПЛАН КУРСУ “ІНФОРМАЦІЙНЕ ПРАВО”

Т Е М А 1 ОСНОВНІ ПОНЯТТЯ І КАТЕГОРІЇ ІНФОРМАЦІЙНОГО ПРАВА

Цілі і завдання курсу. Інформація як категорія інформаційного права. Загальні та юридичні властивості інформації. Розвиток технологій обробки інформації та їх вплив на інформаційні процеси. Основні риси сучасного інформаційного суспільства. Програмні нормативно-правові акти щодо формування інформаційного суспільства.

Т Е М А 2 ПРЕДМЕТ, МЕТОД І СИСТЕМА ІНФОРМАЦІЙНОГО ПРАВА

Предмет інформаційного права. Метод інформаційного права. Поняття, система та джерела інформаційного права. Класифікація інформації згідно з національним законодавством (види та галузі інформації). Поняття і структура інформаційних правовідносин. Інформаційний простір та інформаційний суверенітет.

Т Е М А 3 ГАРАНТІЇ ПРАВ І СВОБОД ЛЮДИНИ У СФЕРІ ІНФОРМАЦІЇ

Міжнародно-правові стандарти прав людини в інформаційній сфері та їх класифікація. Право на інформацію. Право на свободу слова. Право на конфіденційність приватного життя. Конституційні засади прав і свобод людини в інформаційній сфері. Підстави та випадки обмеження прав людини у сфері інформації.

Т Е М А 4 ОСНОВНІ НАПРЯМИ РЕАЛІЗАЦІЇ ПРАВ І СВОБОД ЛЮДИНИ В СФЕРІ ІНФОРМАЦІЇ

Право громадян на звернення за наданням інформації. Доступ до правової інформації. Доступ до екологічної інформації. Інформаційні права громадян як суб'єктів виборчого процесу. Захист персональних даних.

ТЕМА 5

ПРАВОВІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Історія формування категорій національна безпека та “національні інтереси”. Поняття національних інтересів та національної безпеки. Поняття та правові основи інформаційної безпеки України. Напрями державної політики у сфері інформаційної безпеки. Інституціональний механізм інформаційної безпеки. Міжнародно-правові основи інформаційної безпеки.

ТЕМА 6

ПРАВОВІ РЕЖИМИ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНИХ РЕСУРСІВ

Поняття інформаційних ресурсів. Правовий режим інформаційних ресурсів. Режим доступу до інформації, поняття і зміст. Відкрита інформація та інформація з обмеженим обігом. Основні принципи правого регулювання обігу інформації. Обмеження щодо розповсюдження інформації.

ТЕМА 7

ДЕРЖАВНА ТАЄМНИЦЯ

Поняття та правовий режим державної таємниці. Державні експерти з питань таємниць. Порядок віднесення інформації до державної таємниці. ЗВДТ. Класифікація видів секретної інформації. Засекречування матеріальних носіїв інформації. Доступ та допуск до державної таємниці. Міжнародні передачі таємної інформації.

ТЕМА 8

КОНФІДЕНЦІЙНА ІНФОРМАЦІЯ

Конфіденційна інформація, що перебуває у власності держави. Порядок надання матеріальним носіям інформації грифу ДСК. Обов'язки посадових осіб та службовців у роботі з матеріалами ДСК. Комерційна таємниця. Інформація, що не може бути комерційною таємницею. Організація та правове забезпечення захисту комерційної таємниці. Обов'язки органів публічної влади, щодо захисту комерційної таємниці. Загальні ознаки професійної таємниці. Адвокатська, лікарська таємниця, таємниця страхування та вчинення нотаріальних дій. Банківська таємниця. Підстави та випадки надання доступу до інформації, що становить банківську таємницю

ТЕМА 9**ПРАВОВІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ**

Основні принципи діяльності із захисту інформації. Захист інформації в інформаційних системах. Технічний захист інформації. Криптографічний захист інформації. Ліцензування та атестація робіт із захисту інформації. Ліцензування господарської діяльності з розроблення, виготовлення спеціальних технічних засобів негласного отримання інформації і торгівлі ними. Національна система конфіденційного зв'язку. Державна служба спеціального зв'язку та захисту інформації України.

ТЕМА 10**ПРАВОВЕ РЕГУЛЮВАННЯ ЗАСОБІВ
ТЕЛЕКОМУНІКАЦІЇ**

Основні моделі правового регулювання інформаційної діяльності. Класифікація видів інформаційної діяльності. Міжнародно-правові основи регулювання телекомунікаційних послуг. Міжнародний союз електрозв'язку. Генеральна угода з торгівлі послугами. Правове регулювання використання радіочастот. Національна таблиця розподілу радіочастот. План використання радіочастотного ресурсу України. Розподіл номерного ресурсу. Регулювання ринку телекомунікацій. Національна комісія з питань регулювання зв'язку України.

ТЕМА 11**ПРАВОВЕ РЕГУЛЮВАННЯ ФУНКЦІОНУВАННЯ
ІНТЕРНЕТ**

Основні поняття і принципи, пов'язані з функціонуванням Інтернет, визначені в національному законодавстві. Суб'єкти і об'єкти правовідносин, які виникають щодо функціонування Інтернет. Правові основи адміністрування домену UA. Декларація Ради Європи “Про свободу спілкування в Інтернет”. Національна програма інформатизації. Електронні документи та електронний документообіг. Концепція створення “електронного уряду”. Національний реєстр електронних інформаційних ресурсів.

ТЕМА 12

ПРАВОВЕ РЕГУЛЮВАННЯ ДІЯЛЬНОСТІ ДРУКОВАНИХ ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ

Політико-правовий контекст діяльності у сфері масової інформації. Правові основи створення та діяльності друкованих ЗМІ. Умови та порядок державної реєстрації друкованих ЗМІ. Суб'єкти діяльності у сфері друкованих ЗМІ та їх правовий статус. Правовий статус журналіста. Правові основи видавничої справи. Суб'єкти видавничої справи. Про Державний реєстр видавців, виготівників і розповсюджувачів видавничої продукції. Правові основи діяльності інформаційних агентств. Державна реєстрація інформаційних агентств.

ТЕМА 13

ПРАВОВЕ РЕГУЛЮВАННЯ ДІЯЛЬНОСТІ ЕЛЕКТРОННИХ ЗМІ

Правові основи діяльності електронних ЗМІ. Структура та повноваження Національної ради України з питань телебачення і радіомовлення. Порядок ліцензування каналів мовлення та умови конкурсу на отримання ліцензій. Державний реєстр телерадіоорганізацій України. Візуальні позначки класифікації відеопродукції. Сутність і структура прав на демонстрацію і розповсюдження фільмів. Державне посвідчення на право розповсюдження і демонстрування фільмів. Державний реєстр виробників, розповсюджувачів і демонстраторів фільмів. Державна служба кінематографії. Індекси обмеження демонстрації та розповсюдження.

ТЕМА 14

ПРАВОВЕ РЕГУЛЮВАННЯ БІБЛІОТЕЧНОЇ ТА АРХІВНОЇ СПРАВИ

Правові основи бібліотечної справи. Суб'єкти діяльності в галузі бібліотечної справи. Доступ до інформації в бібліотечній справі. Правове регулювання архівної справи. Суб'єкти правових відносин у галузі архівної справи. Правовий режим архівів. Комплектування, зберігання та облік архівних фондів. Порядок доступу до інформації в архівних фондах.

ТЕМА 15

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ УПРАВЛІНСЬКОЇ ДІЯЛЬНОСТІ

Інформація як складова управлінської діяльності. Поняття інформаційного забезпечення управлінської діяльності. Інформатизація державного управління згідно із Концепцією адміністративної реформи. Інформаційне забезпечення роботи Верховної Ради України. Інформаційні ресурси органів виконавчої влади.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

СПЕЦІАЛЬНА ЛІТЕРАТУРА

1. Адміністративне право України. Академічний курс. / За ред. В.Б. Авер'янова. – К., 2004.
2. Адміністративне право України / За ред. С. Ківалова. – Одеса: Юридична літ-ра, 2003.
3. Адміністративне право України / За ред. Ю.П. Битяка. – К.: Юрінком-інтер, 2006.
4. *Арістова І.В.* Державна інформаційна політика: організаційно-правові аспекти. — Харків: УВС, 2000.
5. *Бандурка О.М., Тищенко Н.М.* Адміністративний процес. – К., 2001.
6. *Баранов О.А.* Інформаційне право України: стан, проблеми, перспективи. – К.: СофтПрес, 2005.
7. *Бачило И.Л.* Информационное право. Основы практической информатики. – М., 2001.
8. *Бачило И.Л., Лопатин В.Н., Федотов М.А.* Информационное право. –СПб., 2001.
9. *Бахрах Д. Н.* Административное право: Учеб. для вузов. – М.: БЕК, 1999.
10. *Бернард Г. Сіган.* Створення конституції для народу чи республіки, що здобули свободу. – К.: Ін-т демократії ім. П. Орлика, 1993.
11. *Васильюк В.Я., Климчик С.О.* Інформаційна безпека держави: Курс лекцій. – К., 2008.
12. *Венгеров А.Б.* Право и информация в условиях автоматизации управления. – М., 1978.
13. *Винер Н.* Кибернетика и управление, их связь в животном и машине. – М.: Иностран. Лит-ра, 1958.
14. *Виноградова Г.В.* Інформаційне право України: Навч. посібник. – К.: МАУП, 2006.
15. *Гаврилов О.А.* Курс правовой информатики. – М.: Изд-во НОРМА, 2000.
16. *Гостев И.М.* Информационное право в России. // Конфидент. – 2000. – № 1–2.
17. Доступ до інформації та електронне урядування. – К.: Факт, 2004.
18. Європа на шляху до інформаційного суспільства // Матеріали Європейської Комісії 1994 – 1995 рр. – К.: Держкомзв'язку та інформатизації України, 2000.
19. Е-майбутнє та інформаційне право / За ред. М. Швеця. – К., 2006.
20. Інформаційна відкритість органів державної влади України / За ред. М. Лациби. – К., 2005.
21. Інформаційне забезпечення управлінської діяльності в умовах інформатизації. Організаційно-правові питання теорії і практики / За ред. Р.А. Калюжного та В.О. Шамрая. – К., 2002.

22. Інформаційне законодавство: Зб. законодавчих актів: У 6 т. – К.: Юрид. думка, 2005.
23. Інформація, зв'язок і телекомунікації в Україні: економіка, право, управління. / За ред. С.О. Довгого, Б.І. Холод – К.: Укртелеком, 2001.
24. *Інформация*. Дипломатия. Психология. – М.: Известия, 2002.
25. *Кастельс М.* Информационная эпоха: экономика, общество, культура. Пер. с англ. под науч. ред. О.И. Шкаратана – М.: ГУ ВШЭ, 2000.
26. *Копылов В.А.* Информационное право. – М.: Юристъ, 1997.
27. *Копылов В.А.* Информационное право. – 2-е изд., перераб. и доп. – М.: Юристъ, 2002.
28. *Кормич Б.А.* Інформаційна безпека: організаційно-правові основи: Навч. посібник. – К.: Кондор, 2004.
29. *Кормич Б.А.* Інформація як категорія інформаційного права // Актуальні проблеми держави і права. Зб. наук. праць – Вип. 16. – Одеса: Юрид. літ-ра, 2002. – с. 367 – 374.
30. *Кормич Б.А.* Організаційно-правові засади політики інформаційної безпеки України. – Одеса: Юрид. літ-ра, 2003.
31. *Крос К., Гакет Р.* Політична комунікація і висвітлення новин у демократичних суспільствах. Перспективи конкуренції. – К.: Основи, 2000.
32. *Курушин В.Д., Минаев В.А.* Компьютерные преступления и информационная безопасность: Справ. – М.: Новый юрист, 1998.
33. *Ліпкан В.А., Максименко Ю.Є., Желіховський В.М.* Інформаційна безпека України в умовах євроінтеграції. – К.: КНТ, 2006.
34. *Литвиненко О.В.* Інформаційна безпека Європи. – К., 1999.
35. *Марущак А.І.* Інформаційне право: Доступ до інформації: Навч. посібник. – К.: КНТ, 2007.
36. Новая постиндустриальная волна на Западе. Антология. – М.: Academia, 1999.
37. Огляд практики Європейського суду з прав людини. Норми та стандарти Конвенції про захист прав і основних свобод людини. – К.: Мін-во юстиції України, 2002.
38. Основи інформаційного права України. – К.: Знання, 2004.
39. Організаційно-правові основи захисту інформації з обмеженим доступом / За ред. В.С. Сідака. – К.: Вид-во Європейського ун-ту, 2006.
40. Правове забезпечення інформаційної діяльності в Україні / За ред. Ю.С. Шемшученка, І.С. Чижа – К.: Юрид. думка, 2006.
41. *Рабінович П.М., Панкевич І.М.* Здійснення прав людини: проблеми обмежування (загальнотеоретичні аспекти). – Л., 2001.
42. *Рассолов М.М.* Информационное право. – М., Юристъ, 1999.
43. *Северин В.А.* Правовое обеспечение информационной безопасности предприятия. – М., 2000.
44. Стратегія національної безпеки України в контексті досвіду світової спільноти: Зб. ст. за матер. міжнар. конф. – К.: Сатсанга, 2001.

45. Хрипко С.Л. Інформаційне право: Навч.-метод. посібник. – Донецьк, 2005.
46. Шеннон К.Е. Работы по теории информации и кибернетике. – М., 1963.
47. Шиллер Г. Манипуляторы сознанием. – М.: Мысль, 1980.
48. Ярочкин В.И. Информационная безопасность. – М.: Междунар. отношения, 2000.
49. Ярочкин В.И. Информационная безопасность: Учебник. – М.: Фонд «Мир», 2003.
50. Annual Information Society Report 2007 A European Information Society for Growth and Employment / COM (2007) 146. SEC (2007) 395. – Volumes 1,2,3 – March 2007.

НОРМАТИВНО-ПРАВОВІ АКТИ

Закони України

51. Конституція України. Прийнята Верховною Радою України 28 червня 1996 року // Відомості Верховної Ради України. – 1996. – №30 – Ст. 141.
52. Кримінальний кодекс України від 5 квітня 2001 р. // Відомості Верховної Ради України. – 2001. – № 25-26 – Ст. 131.
53. Основи законодавства України про культуру: Закон України від 14 лютого 1992 р. № 2117-XII // Відомості Верховної Ради України. – 1992. – № 21. – Ст. 294.
54. Основи законодавства України про охорону здоров'я: Закон України від 19 листопада 1992 р. № 2801-XII // Відомості Верховної Ради України. – 1993. – № 4. – Ст. 19.
55. Про адвокатуру: Закон України від 19 грудня 1992 р. № 2887-XII // Відомості Верховної Ради України. – 1993. – № 9. – Ст. 62.
56. Про банки і банківську діяльність: Закон України від 7 грудня 2000 року № 2121-III // Відомості Верховної Ради України. – 2001. – № 5-6. – Ст. 30.
57. Про бібліотеки і бібліотечну справу: Закон України від 27 січня 1995 р. // Відомості Верховної Ради України. – 1995. – № 7. – ст. 45.
58. Про вибори народних депутатів України: Закон України в редакції Закону № 2777-IV від 7 липня 2005 р. // Відомості Верховної Ради України. – 2005. – № 38-39. – Ст. 449.
59. Про видавничу справу: Закон України від 5 червня 1997 р. № 318/97-ВР // Відомості Верховної Ради України. – 1997. – № 32. – Ст. 206.
60. Про державну службу: Закон України від 16 грудня 1993 року № 3723-XII // Відомості Верховної Ради України. – 1993. – № 52. – Ст. 490.
61. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23 лютого 2006 р. № 3475-IV // Відомості Верховної Ради України. – 2006. – № 30. – Ст. 258.
62. Про державну статистику: Закон України від 17 вересня 1992 р. // Відомості Верховної Ради України. – 1992. – № 43. – Ст.608 (В редакції Закону № 1922-III від 13.07.2000 / ВВР, 2000. - № 43. – Ст. 362)

63. Про державну тасмницю: Закон України від 21 січня 1994 року № 3855-ХІІ // Відомості Верховної Ради України. – 1994. – № 16. – Ст. 93. (В редакції Закону № 1079-ХІV від 21.09.99).
64. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16 листопада 1992 р. № 2782-ХІІ // Відомості Верховної Ради України. – 1993. – № 1. – Ст. 1.
65. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 31 травня 2005 р. № 2594-IV // Відомості Верховної Ради України. – 2005. – № 26. – Ст. 347.
66. Про захист суспільної моралі: Закон України від 20 листопада 2003 р. № 1296-IV // Відомості Верховної Ради України. – 2004. – № 14. – Ст. 192.
67. Про звернення громадян: Закон України від 2 жовтня 1996 р. № 393/96-ВР // Відомості Верховної Ради України – 1996. – № 47. – Ст. 256.
68. Про зону надзвичайної екологічної ситуації: Закон України від 13 липня 2000 р. № 1908-ІІІ. // Відомості Верховної Ради України. – 2000. – № 42. – Ст. 348.
69. Про електронні документи та електронний документообіг: Закон України від 22 травня 2003 р. № 851-IV // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 275.
70. Про електронний цифровий підпис: Закон України від 22 травня 2003 р. № 852-IV // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 276.
71. Про інформацію: Закон України від 2 жовтня 1992 р. № 2657-ХІІ // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.
72. Про інформаційні агентства: Закон України від 28 лютого 1995 р. № 74/95-ВР // Відомості Верховної Ради України. – 1995. – № 13. – Ст. 83.
73. Про Концепцію Національної програми інформатизації: Закон України від 4 лютого 1998 року № 75/98-ВР // Відомості Верховної Ради України. – 1998. – № 27-28. – Ст. 182.
74. Про науково-технічну інформацію: Закон України від 25 червня 1993 р. № 3322-ХІІ // Відомості Верховної Ради України. – 1993. – № 33. – Ст. 345.
75. Закон України «Про наукову і науково-технічну експертизу» від 10 лютого 1995 р. № 51/95-ВР // Відомості Верховної Ради України. – 1995. – № 9. – Ст. 56.
76. Про Національний архівний фонд та архівні установи: Закон України від 24 грудня 1993 р. № 3814-ХІІ // Відомості Верховної Ради України. – 1994. – № 15. – Ст. 86.
77. Про Національну програму інформатизації: Закон України від 4 лютого 1998 р. № 74/98-ВР // Відомості Верховної Ради України. – 1998. – № 27-28. – Ст. 18.
78. Про Національну раду України з питань телебачення і радіомовлення: Закон України від 23 вересня 1997 р. № 538/97-ВР // Відомості Верховної Ради України. – 1997. – № 48. – Ст. 296.

79. Про Національну систему конфіденційного зв'язку: Закон України від 10 січня 2002 р. № 2919-III // Відомості Верховної Ради України – 2002 – № 15. – Ст. 103.
80. Про інформаційні агентства: Закон України від 28 лютого 1995 р. № 74/95-ВР // Відомості Верховної Ради України. – 1995. – № 13. – Ст. 83.
81. Про обов'язковий примірник документів: Закон України від 9 квітня 1999 р. № 595-XIV // Відомості Верховної Ради України. – 1999. – № 22-23. – Ст. 199.
82. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135-XII. // Відомості Верховної Ради. – 1992. – № 22. – ст. 303.
83. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 9 січня 2007 р. № 537-V // Відомості Верховної Ради України – 2007. – № 12. – Ст. 102.
84. Про основи національної безпеки України: Закон України від 19 червня 2003 р. № 964 – IV // Офіційний вісник України. – № 29. – с. 38. – Ст. 1433.
85. Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації: Закон України від 23 вересня 1997 р. № 539/97-ВР // Відомості Верховної Ради України. – 1997. – № 49. – Ст. 299.
86. Про порядок ввезення (пересилання) в Україну, митного оформлення й оподаткування особистих речей, товарів та транспортних засобів, що ввозяться (пересилаються) громадянами на митну територію України: Закон України від 13 вересня 2001 р. № 2681-III//Відомості Верховної Ради України. – 2002. – № 1. – Ст. 2
87. Про радіочастотний ресурс України: Закон України від 1 червня 2000 р. № 1770-III // Відомості Верховної Ради України. – 2000. – № 36. – Ст. 298.
88. Про Раду національної безпеки і оборони України: Закон України від 5 березня 1998 року № 183/98-ВР // Відомості Верховної Ради України. – 1998. – № 35. – Ст. 237.
89. Про ратифікацію Статуту і Конвенції Міжнародного союзу електров'язку: Закон України від 15 липня 1994 р. № 116/94-ВР // Відомості Верховної Ради України. – 1994. – № 33. – Ст. 306.
90. Про рекламу: Закон України від 3 липня 1996 р. № 270/96-ВР // Відомості Верховної Ради України. – 1996. – № 39. – Ст. 181.
91. Про Службу безпеки України: Закон України від 25 березня 1992 р. № 2229-XII // Відомості Верховної Ради України. – 1992. – № 27. – Ст. 382.
92. Про службу в органах місцевого самоврядування: Закон України від 7 червня 2001 року № 2493-III // Відомості Верховної Ради України. – 2001. – № 33. – Ст. 175.
93. Про систему Суспільного телебачення і радіомовлення України: Закон України від 18 липня 1997 р. № 485/97-ВР // Відомості Верховної Ради України. – 1997. – № 45. – Ст. 284.

94. Про страхування: Закон України від 7 березня 1996 р. № 85/96-ВР // Відомості Верховної Ради України. – 1996. – № 18. – Ст. 78.
95. Про телебачення і радіомовлення: Закон України від 21 грудня 1993 р. № 3759-ХІІ // Відомості Верховної Ради України. – 1994. – № 10. – Ст. 43.
96. Про телекомунікації: Закон України від 18 листопада 2003 р. № 1280-ІV // Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155.
97. Про Центральну виборчу комісію: Закон України від 30 червня 2004 р. № 1932-ІV // Відомості Верховної Ради України. – 2004. – № 36. – Ст. 448.
98. Цивільний кодекс України № 435-ІV від 16 січня 2003 р. // Відомості Верховної Ради України. – 2003. – №№ 40 – 44. – Ст. 356.

Постанови Верховної Ради України

99. Про Регламент Верховної Ради України: Постанова Верховної Ради України від 16 березня 2006 р. № 3547-ІV // Відомості Верховної Ради України – 2006. – № 23, № 24-25. – Ст. 202.
100. Про Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні: Постанова Верховної Ради України від 1 грудня 2005 р. № 3175-ІV // Відомості Верховної Ради України. – 2006. – № 15. – Ст. 131.

Рішення Конституційного Суду України

101. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К.Г. Устименка) від 30 жовтня 1997 року № 5-зп. – Справа № 18/203-97.
102. Рішення Конституційного Суду України у справі за конституційним поданням 55 народних депутатів України щодо відповідності Конституції України (конституційності) положень частин другої, третьої статті 17, частин першої, дев'ятої статті 20 Закону України «Про телекомунікації», статті 2 Указу Президента України «Про Національну комісію з питань регулювання зв'язку України» від 8 жовтня 2008 р. № 21-рп/2008 – Справа № 1-42/2008.

Укази Президента України

103. Питання Апарату Ради національної безпеки і оборони України: Указ Президента України від 14 жовтня 2005 р. № 1446/2005
104. Про Воєнну доктрину України: Указ Президента України від 15 червня 2004 р. № 648/2004.
105. Про додержання прав людини під час проведення оперативно-технічних заходів: Указ Президента України від 7 листопада 2005 р. № 1556/2005.
106. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні: Указ Президента України від 31 липня 2000 р. № 928/2000.

107. Про Національну комісію з питань регулювання зв'язку України: Указ Президента України від 21 серпня 2004 р. № 943/2004.
108. Про Перелік посадових осіб, на яких покладається виконання функцій державного експерта з питань таємниць: Указ Президента України від 29 травня 2006 р. № 452/2006.
109. Про Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ Президента України від 22 травня 1998 р. № 505/98.
110. Про Положення про технічний захист інформації в Україні: Указ Президента України від 27 вересня 1999 р. № 1229.
111. Про порядок офіційного оприлюднення нормативно-правових актів та набрання ними чинності: Указ Президента України від 10 червня 1997 р. № 503/97. (В редакції Указу Президента України №1235/98 від 10 листопада 1998 р.)
112. Про Стратегію національної безпеки України: Указ Президента України від 12 лютого 2007 р. № 105/2007.

Постанови Кабінету Міністрів України

113. Деякі питання організації діяльності Державної служби спеціального зв'язку та захисту інформації: Постанова Кабінету Міністрів України від 24 червня 2006 р. № 869.
114. Питання Адміністрації Державної служби спеціального зв'язку та захисту інформації: Постанова Кабінету міністрів України від 25 травня 2006 р. № 734.
115. Питання Державної служби кінематографії: Постанова Кабінету Міністрів України від 7 березня 2006 р. № 251.
116. Про Державний реєстр видавців, виготівників і розповсюджувачів видавничої продукції: Постанова Кабінету Міністрів України від 28 вересня 1998 р. № 1540.
117. Про затвердження Інструкції з діловодства за зверненнями громадян в органах державної влади і місцевого самоврядування, об'єднаннях громадян, на підприємствах, в установах, організаціях незалежно від форм власності, в засобах масової інформації: Постанова Кабінету Міністрів України від 14 квітня 1997 р. № 348.
118. Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави: Постанова Кабінету Міністрів України від 27 листопада 1998 р. № 1893.
119. Про затвердження Національної таблиці розподілу смуг радіочастот України: Постанова Кабінету Міністрів України від 15 грудня 2005 р. № 1208.
120. Про затвердження Плану використання радіочастотного ресурсу України: Постанова Кабінету Міністрів України від 9 червня 2006 р. № 815.
121. Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації: Постанова Кабінету Міністрів України від 24 червня 2006 р. № 868.

122. Про затвердження Положення про державне посвідчення на право розповсюдження і демонстрування фільмів: Постанова Кабінету Міністрів України від 17 серпня 1998 р. № 1315.
123. Про затвердження Положення про Державний реєстр виробників, розповсюджувачів і демонстраторів фільмів: Постанова Кабінету Міністрів України від 14 січня 2004 р. № 27.
124. Про затвердження Положення про Міністерство культури і туризму України: Постанова Кабінету Міністрів України від 8 листопада 2006 р. № 1566.
125. Про затвердження Положення про Національний реєстр електронних інформаційних ресурсів: Постанова Кабінету Міністрів України від 17 березня 2004 р. № 326.
126. Про затвердження Положення про Національну комісію з питань регулювання зв'язку України: Постанова Кабінету Міністрів України від 25 липня 2007 р. № 971.
127. Про затвердження Положення про центральний засвідчувальний орган: Постанова Кабінету Міністрів України від 28 жовтня 2004 р. № 1451.
128. Про затвердження Порядку акредитації центру сертифікації ключів: Постанова Кабінету Міністрів України від 13 липня 2004 р. № 903.
129. Про затвердження Порядку ведення Єдиного державного реєстру нормативно-правових актів та користування ним: Постанова Кабінету Міністрів України від 23 квітня 2001 р. № 376.
130. Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності: Постанова Кабінету Міністрів України від 28 жовтня 2004 р. № 1452.
131. Про затвердження Порядку підключення до глобальних мереж передачі даних: Постанова Кабінету Міністрів України від 12 квітня 2002 р. № 522.
132. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373.
133. Про заходи щодо створення електронної інформаційної системи «Електронний Уряд»: Постанова Кабінету Міністрів України від 24 лютого 2003 р. № 208.
134. Про Національну експертну комісію України з питань захисту суспільної моралі: Постанова Кабінету Міністрів України від 17 листопада 2004 р. № 1550.
135. Про перелік відомостей, що не становлять комерційної таємниці: Постанова Кабінету Міністрів України від 9 серпня 1993 р. № 611.
136. Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади: Постанова Кабінету Міністрів України від 4 січня 2002 р. № 3.

137. Про адміністрування домену «UA»: Розпорядження Кабінету Міністрів України від 22 липня 2003 р. N 447-р.
138. Про затвердження Концепції формування системи національних електронних інформаційних ресурсів: Розпорядження Кабінету Міністрів України від 5 травня 2003 р. № 259-р.
139. Про створення спеціальної мережі стільникового зв'язку Національної системи конфіденційного зв'язку: Розпорядження Кабінету Міністрів України від 24 вересня 2005 р. № 405-р.

Нормативно-правові акти інших органів державної влади

140. Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб: Наказ ДСТСЗІ СБУ від 23 лютого 2002р. № 9.
141. Про затвердження Загальних правил поведінки державного службовця: Наказ Головного управління державної служби України № 58 від 23 жовтня 2000 р.
142. Про затвердження Зводу відомостей, що становлять державну таємницю: Наказ Служби Безпеки України від 12 серпня 2005 р. № 440.
143. Про затвердження зобов'язання громадянина України у зв'язку з допуском до державної таємниці та анкети для оформлення допуску до державної таємниці: Наказ Служби Безпеки України № 190 від 18 червня 2001 р. Про затвердження Інструкції про порядок здійснення Службою безпеки України контролю за обігом документів, які містять конфіденційну інформацію, що є власністю держави: Наказ Служби безпеки України 17 липня 2006 р. № 550.
144. Про затвердження Інструкції про порядок та умови одержання інформації з інформаційного фонду Єдиного державного реєстру нормативно-правових актів: Наказ Міністерства юстиції України від 26 червня 2002 р. № 57/5.
145. Про затвердження конкурсних умов: Рішення Національної ради України з питань телебачення і радіомовлення від 21 березня 2007 р. № 350.
146. Про затвердження ліцензійних умов провадження господарської діяльності, пов'язаної з розробленням, виробництвом, впровадженням, обслуговуванням, дослідженням ефективності систем і засобів технічного захисту інформації, наданням послуг у галузі технічного захисту інформації: Спільний наказ Держкомпідприємництва та ДСТСЗІ СБУ від 29 грудня 2000 р. № 89/67.
147. Про затвердження Національного плану нумерації України: Наказ Міністерства транспорту і зв'язку України від 23 листопада 2006 р. № 1105.
148. Про затвердження Переліку конфіденційної інформації: Наказ Міністерства палива та енергетики України від 15 липня 2006 р. № 288.

149. Про затвердження Порядку проведення робіт з сертифікації засобів забезпечення технічного захисту інформації загального призначення: Наказ Держстандарту України від 9 липня 2001 р. № 329/32.
150. Про затвердження Положення про державну експертизу в сфері технічного захисту інформації: Наказ ДСТСЗІ СБУ від 29 грудня 1999 р. № 62.
151. Про затвердження Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації: Наказ ДСТСЗІ СБУ 30 листопада 1999 р. № 53.
152. Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах: Наказ ДСТСЗІ СБУ від 24 грудня 2001 р. № 76.
153. Про затвердження Положення про порядок роботи зі зверненнями громадян і організації їх особистого прийому в системі Міністерства внутрішніх справ України: Наказ МВС України від 10 жовтня 2004 р. № 1177.
154. Про затвердження Положення про державну реєстрацію фільмів: Наказ Мінкультури від 31 серпня 2004 р. № 571.
155. Про затвердження Положення про порядок надання екологічної інформації: Наказ Мінприроди України від 18 грудня 2003 р. № 169.
156. Про затвердження Положення про участь громадськості у прийнятті рішень у сфері охорони довкілля: Наказ Мінприроди України від 18 грудня 2003 р. № 168.
157. Про затвердження Положення про щоквартальне інформування населення через ЗМІ про об'єкти, які є найбільшими забруднювачами навколишнього природного середовища: Наказ Мінприроди України від 1 листопада 2005 р. № 397.
158. Про затвердження Положення про експертні комісії з питань державної таємниці: Наказ Служби Безпеки України від 14 грудня 2004 р. № 696.
159. Про затвердження Положення про Державну інспекцію зв'язку: Рішення Національної комісії з питань регулювання зв'язку України від 2 серпня 2007 р. № 875.
160. Про затвердження Положення про державну реєстрацію друкованих засобів масової інформації в Україні та Положення про державну реєстрацію інформаційних агентств як суб'єктів інформаційної діяльності: Наказ Міністерства юстиції України від 21 лютого 2006 р. № 12/5.
161. Про затвердження Положення про державну реєстрацію інформаційних агентств як суб'єктів інформаційної діяльності: Наказ Міністерства юстиції України від 21 лютого 2006 р. № 12/5.
162. Про затвердження Порядку здійснення державного нагляду за ринком телекомунікацій: Рішення Національної комісії з питань регулювання зв'язку України від 27 жовтня 2006 р. № 426.
163. Про затвердження Порядку проведення державної реєстрації електронних інформаційних ресурсів: Наказ Міністерства транспорту та зв'язку України від 27 березня 2005 № 153.

164. Про затвердження Правил зберігання, захисту, використання та розкриття банківської таємниці: Постанова Національного банку України від 14 липня 2006 р. № 267.
165. Про затвердження системи візуальних позначок класифікації кіновідеопродукції залежно від аудиторії, на яку вона розрахована: Рішення Національної ради України з питань телебачення і радіомовлення від 18 червня 2003 р. № 781.
166. Про затвердження Тимчасової інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації: Наказ Держстандарту України та Служби безпеки України від 28 листопада 1997 р. № 708/156.
167. Про затвердження Типового положення про правову громадську приймальню: Наказ Міністерства юстиції України від 15 червня 2005 р. № 61/5.
168. Про питання захисту авторських прав в Інтернеті: Постанова Вищого Арбітражного Суду України від 5 червня 2000 р. № 04-1/5-7/82. // Вісник господарського судочинства. – 2001. – № 2.
169. Про положення про веб-сайт Верховної Ради України у глобальній інформаційній мережі Інтернет: Розпорядження Голови Верховної Ради України від 24 травня 2001 р. № 462.
170. Про Перелік автоматизованих систем інформаційно-технологічного забезпечення діяльності Верховної Ради України: Розпорядження Голови Верховної Ради України від 1 липня 2003 року № 663.
171. Регламент Національної комісії з питань регулювання зв'язку України: Рішення Національної комісії регулювання зв'язку України від 17 травня 2005 р. № 1.

Міжнародно-правові акти

172. Генеральна угода з торгівлі послугами 1994 р. / Україна і Світова організація торгівлі: Збірник офіційних документів. – К., 2002.
173. Господарський кодекс України від 16 січня 2003 р. // Відомості Верховної Ради України. – 2003. – № 18. – Ст. 144.
174. Декларація принципів Побудова інформаційного суспільства - глобальне завдання в новому тисячоріччі. Женева. 12 грудня 2003 р.
175. Декларация руководящих принципов по использованию вещания через спутники для свободного распространения информации, развития образования и расширения культурных обменов. ЮНЕСКО. 15 ноября 1972 г.
176. Декларация тысячелетия Организации Объединенных Наций. Затверджена резолюцією 55/2 Генеральної Асамблеї ООН від 8 вересня 2000 р. // A/RES/55/2.
177. Загальна декларація прав людини. Прийнята Генеральною Асамблеєю ООН 10 грудня 1948 р. /Док.ООН/PES/217 А.
178. Конвенція про доступ до інформації, участь громадськості в процесі прийняття рішень та доступ до правосуддя з питань, що стосуються довкілля від 28 червня 1998 р. (Ратифіковано Законом України № 832-XIV

- від 6 липня 1999 р.) // Відомості Верховної Ради України. – 1999. – № 34. – Ст. 296.
179. Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру. Страсбург, 28 січня 1981 р. / Збірка договорів Ради Європи. – Київ: Парламентське видавництво, 2000.
180. Конвенція про захист прав і основних свобод людини 1950 року, Перший протокол та протоколи № 1, 4, 6, 7, 9, 10 та 11 до Конвенції (Рим, 4.XI.1950) / «Голос України», 10 січня 2001 р. № 3 (2503) – стор. 6 – 8.
181. Конвенція про кіберзлочинність. Рада Європи. Будапешт 23 листопада 2001 р. (Ратифіковано Законом України «Про ратифікацію Конвенції про кіберзлочинність» від 7 вересня 2005 р. № 2824-IV).
182. Міжнародний пакт про громадянські і політичні права. Прийнято 16 грудня 1966 р. Генеральною Асамблеєю ООН. Док. ООН A/RES/2200 A (XXI).
183. Рада Європи. Європейська конвенція про транскордонне телебачення ETS № 132. Страсбург. 5 травня 1989 р.
184. Соглашение о правовом режиме информационных ресурсов Пограничных войск государств-участников Содружества Независимых Государств (Москва, 25 ноября 1998 г.) // Содружество. Информационный вестник Совета глав государств и Совета глав правительств СНГ. – № 3(30). – С. 299 - 304.
185. Соглашение о создании Регионального содружества в области связи. Подписано в г. Москва. 17 декабря 1991 г.
186. Угода між Кабінетом Міністрів України та Урядом Федеративної Республіки Німеччина про взаємний захист таємної інформації від 29 травня 1998 р. (Затверджено Постановою Кабінету Міністрів України № 1433 від 14.09.98).
187. Угода між Урядом України та Урядом Французької Республіки про взаємну охорону таємної інформації та матеріалів від 7 грудня 1999 року. (Схвалено і подано на ратифікацію Постановою Кабінету Міністрів № 468 від 06.05.2001).
188. Хартия Глобального информационного общества. Принята 22 июля 2000 г., Окинава. // Информация. Дипломатия. Психология. – М.: Известия, 2002.
189. COUNCIL RESOLUTION of 22 March 2007 on a Strategy for a Secure Information Society in Europe // Official Journal of the European Union C 68, 24.3.2007.
190. Declaration on freedom of communication on the Internet. Adopted by the Committee of Ministers at the 840th meeting of the Ministers' Deputies. Strasbourg, 28.05.2003./ <http://www.coe.int/portalT.asp>
191. i2010 – A European Information Society for growth and employment, COM(2005) 229.
192. United Nations. A/RES/56/19 “Developments in the field of information and telecommunications in the context of international security” Resolution Adopted By The General Assembly. 7 January 2002.

Зміст

Передмова.....	3
----------------	---

ЗАГАЛЬНА ЧАСТИНА

РОЗДІЛ І

ПРИНЦИПОВІ ЗАСАДИ ІНФОРМАЦІЙНОГО ПРАВА

Глава 1. Основні поняття та категорії інформаційного права	5
1.1. Інформація як категорія інформаційного права	5
1.2. Загальні та юридичні властивості інформації	12
1.3. Розвиток технологій обробки інформації та їх вплив на інформаційні процеси.....	15
1.4. Основні риси сучасного інформаційного суспільства	17
1.5. Програмні нормативно-правові акти щодо формування інформаційного суспільства	26
Глава 2. Предмет, метод та система інформаційного права	33
2.1. Предмет інформаційного права	33
2.2. Метод інформаційного права	38
2.3. Поняття, система та джерела інформаційного права	41
2.4. Класифікація інформації в українському законодавстві	48
2.5. Поняття та структура інформаційних правовідносин	55
2.6. Інформаційний простір та інформаційний суверенітет	59
Глава 3. Гарантії прав і свобод людини в сфері інформації як базис інформаційного права	64
3.1. Міжнародно-правові стандарти прав людини в інформаційній сфері та їх класифікація	64
3.2. Конституційні засади прав і свобод людини в інформаційній сфері	70
3.3. Підстави та випадки обмеження прав людини в сфері інформації.....	78
Глава 4. Основні напрямки реалізації прав і свобод людини в сфері інформаційного права	87
4.1. Право на звернення щодо надання інформації	87
4.2. Доступ до правової інформації.....	89
4.3. Доступ до екологічної інформації.....	94
4.4. Інформаційні права громадян як суб'єктів виборчого процесу	99

4.5. Захист персональних даних	107
Глава 5. Інформаційна безпека	116
5.1. Історія формування категорій національна безпека та національні інтереси	116
5.2. Поняття та правові основи інформаційної безпеки України	127
5.3. Основні напрямки державної політики інформаційної безпеки	133
5.4. Інституціональний механізм інформаційної безпеки	141
5.5. Міжнародно-правові засади інформаційної безпеки	148
Глава 6. Правові режими інформації та інформаційних ресурсів	155
6.1. Поняття та правовий режим інформаційних ресурсів	155
6.2. Режим доступу до інформації, поняття та зміст	160
6.3. Основні принципи правового регулювання обігу інформації	164
6.5. Обмеження щодо розповсюдження інформації	169

ОСОБЛИВА ЧАСТИНА

РОЗДІЛ II

ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ

Глава 7. Державна таємниця	176
7.1. Поняття та правовий режим державної таємниці	176
7.2. Державні експерти з питань таємниці	182
7.3. Порядок засекречування інформації	184
7.4. ЗВДТ. Класифікація видів секретної інформації	187
7.5. Міжнародні передачі таємної інформації	192
Глава 8. Конфіденційна інформація	196
8.1. Конфіденційна інформація, що знаходиться у власності держави	196
8.2. Комерційна таємниця	203
8.3. Професійна таємниця	206
8.4. Банківська таємниця	211
Глава 9. Правові основи захисту інформації	216
9.1. Основні принципи діяльності із захисту інформації	216
9.2. Захист інформації в інформаційних системах	221
9.3. Технічний захист інформації	225
9.4. Криптографічний захист інформації	228

9.5. Національна система конфіденційного зв'язку	231
9.6. Державна служба спеціального зв'язку та захисту інформації України	233

РОЗДІЛ III ІНФОРМАЦІЙНА ДІЯЛЬНІСТЬ

Глава 10. Правове регулювання телекомунікацій	237
10.1. Основні моделі правого регулювання інформаційної діяльності	237
10.2. Міжнародно-правові основи регулювання телекомунікацій	242
10.3. Правове регулювання використання радіочастот	246
10.4. Регулювання ринку телекомунікацій	251
10.5. Національна комісія з питань регулювання зв'язку України	255
Глава 11. Правове регулювання функціонування мережі інтернет	260
11.1. Основні поняття і принципи, пов'язані з функціонуванням Інтернет, визначені в національному законодавстві	260
11.2. Суб'єкти і об'єкти правовідносин, які виникають щодо функціонування Інтернет	264
11.3. Правові основи адміністрування домену "UA"	266
11.4. Декларація Ради Європи "Про свободу спілкування в Інтернет"	268
11.5. Національна програма інформатизації	270
11.6. Електронні документи та електронний документообіг	273
11.7. Концепція створення "електронного уряду"	275
11.8. Національний реєстр електронних інформаційних ресурсів	279
Глава 12. Правове регулювання розповсюдження масової інформації	282
12.1. Політико-правовий контекст діяльності в сфері масової інформації	282
12.2. Друковані засоби масової інформації (преса)	285
12.3. Видавнича справа	289
12.3. Інформаційні агентства	294
12.4. Правові основи діяльності електронних ЗМІ	297
12.5. Розповсюдження і демонстрування фільмів	304
Програма курсу "Інформаційне право"	312
I. Загальні положення	312
II. Навчальний план курсу "Інформаційне право"	313
III. Тематичний план курсу "Інформаційне право"	314
Список рекомендованої літератури	319

Навчальне видання

Борис Анатольович **Кормич**

ІНФОРМАЦІЙНЕ ПРАВО

Підручник

Підписано до друку 06.07.2010. Формат 60 x 84¹/₁₆.

Папір офсетний. Гарнітура Таймс.

Друк офсетний. Умовн. друк. арк. 20,88.

Тираж 1000 прим. Зам. № 46/07.

Фірма “Бурун і К”

61166, Україна, м. Харків, пр. Леніна, 40, к. 509-г. Тел. (057)719-59-83

Свідоцтво: ДК №1419 від 07.07.2003 р.

Видруковано відповідно до якості наданих діапозитивів у друкарні

ПП “Юнісофт”